BITCOIN

Red Pill

O Renascimento Moral, Material e Tecnológico

— 2ª EDIÇÃO —

Renato Amoedo

Alan Schramm

BITCOIN RED PILL

O Renascimento moral, material e tecnológico

2ª edição
2021

RENATO AMOEDO (@renatotrezoitao)
ALAN SCHRAMM (@alan_schramm)

Revisão
Antonio Lucas Ribeiro (@TonyoLucas)
Lázaro Hanyecz (@bitcoinvangeli1)
Mathias (@mattbitcoiner)
Lucas Ribeiro (@LucasRibeiro_RI)

ISBN: 979-8692311566

Agradecimento

Agradecemos a Cátia Regina Raulino, Eliezer de Queiroz Moreira, José Dirceu, Roger Abdelmassih, Eugenio Chipkevitch, Dilma Rousseff, João de Deus e Luiz Inácio, por mostrarem qual o comportamento dominante neste país e qual o nível moral de seus acadêmicos, instituições e dirigentes.

Sobre os autores

Renato Amoedo Nadier Rodrigues possui graduação em Engenharia de Produção Civil pela UNEB (2000-2006) - ocupando a 1ª posição no Enade 2006 - e graduação em Direito pela UFBA (2000-2004) - por aproveitamento extraordinário. Foi aprovado com nota máxima na Especialização em Direito Empresarial na UFBA (2004-2006) e laureado com nota máxima (10 com distinção) no Mestrado em Direito Privado e Econômico da UFBA (2005-2007). Foi Coordenador Adjunto do Curso de Direito da FBB e Professor desta instituição (2005-2007), da UNYAHNA (2006); da FTE (2007-2008); lecionou Direito Comercial como tirocinista, monitor e Professor substituto da UFBA (2008), aprovado em 1º lugar em seleção pública; e lecionou Direito Mercantil, Financeiro e Econômico como Professor Assistente na UFT (2008-2010), aprovado em 1º lugar no concurso público. Cursou o Doutorado em Administração (Finanças Estratégicas) da UPM - depositando tese sobre governança corporativa; assim como o *EMLE - European Master in Law and Economics* na condição de bolsista da Comissão Europeia pelo *"Erasmus Mundus Scholarship"* (1º lugar do mundo na seleção pela categoria A). É Perito Criminal desde 2007 e *bitcoiner* desde 2015.

Endereço para acessar este CV Lattes:
http://lattes.cnpq.br/6778421578122820

Alan Schramm de Lima cursou a *School of Art, Game and Animation SAGA* (2012-2014); possui graduação em Design de Comunicação Visual e Digital pela Universidade Salvador UNIFACS (2012-2016); *Higher Education Course em UX Design* pelo *Politecnico di Milano*-Itália (2019); Empreendedor na área do *Design* digital; Coautor de relatórios da INOVAFLIX (*Cryptoclub*) sobre Bitcoin (2018); Colunista do Portal Livecoins; Interesses por: Filosofia Libertária, Economia Austríaca, Cultura Digital, UI/UX *Design*, tecnologia e inovação.

Endereço para acessar este CV:
https://www.linkedin.com/in/alan-schramm-08878a57/

PATROCINADORES

Agradecemos imensamente aos nossos
patrocinadores
por apoiar este projeto de educação Bitcoin.

**Esta edição contou com o patrocínio
das seguintes empresas:**

Estratégias para lucrar (ainda mais) com Bitcoin e Ethereum

- Você tem Bitcoin ou Ethereum parado numa carteira ou mesmo na exchange?
- Quer rentabilizar (em dólar ou criptomoeda) seus Bitcoins ou Ethereum?
- Quer conhecer as melhores estratégias para investir na Binance e Deribit?
- Tem receio de fazer trading e perder dinheiro?
- Quer aprender a fazer a gestão de risco dos seus investimentos?
- Se respondeu sim a alguma dessas questões, então podemos te ajudar.

Criamos a Serious Money para facilitar o acesso às estratégias que usamos em nossos investimentos, pois são estratégias lucrativas que, infelizmente, muita gente desconhece.

Por isso fazemos questão de oferecer essas estratégias diferenciadas, por meios acessíveis, para que mais pessoas como você possam ter acesso e obter resultados ainda melhores no investimento em criptomoedas.

Deixando claro que não operamos com seu dinheiro, ensinamos a operá-lo com estratégias vencedoras para que não dependa de ninguém (ninguém mesmo!).

A Serious Money é um projeto educacional criado por Christian Guerreiro e Augusto Gonçalves, especialistas em tecnologia da informação com mais de 20 anos de experiência no mercado de tecnologia e investimentos, em especial derivativos (futuros e opções) com criptomoedas.

Entre em contato conosco pelas redes sociais e tire todas as suas dúvidas sobre como podemos te ajudar!

OAB/BA:34.183

Bender Nascimento Banca & Advogados Associados, foi inaugurado nos idos de 2011 pelo Advogado Dr. Helinz Bender dos Santos Nascimento. Especialista em Advocacia Criminal; atua também na área Empresarial, Civil e Tributário. Entusiasta e estudioso das criptomoedas, inovações disruptivas e das relações jurídicas delas decorrente.

Whatsapp: (75) 99178 – 1105
Instagram: @Bendernascimento
Endereço: Av. João Durval Carneiro, 3253. Caseb.
Feira de Santana - Bahia.

Bitcoin é como a eletricidade primitiva. Bruto, perigoso, parece muito volátil e difícil de usar. Com o tempo, vai começar a parecer mais seguro, fácil e normal. Como a eletricidade, ela inspirará e impulsionará novas indústrias inimagináveis. E um dia vamos nos perguntar como é que vivemos sem isso?

@ObiWanKenoBit

Quando um cientista distinto e experiente diz que algo é possível, é quase certeza que tem razão. Quando ele diz que algo é impossível, ele está muito provavelmente errado.
O único caminho para desvendar os limites do possível é aventurar-se um pouco além dele, adentrando o impossível.
Qualquer tecnologia suficientemente avançada é indistinguível da magia.
Leis de Clark

Quanto mais sábia é uma pessoa, mais aborrecimentos ela tem; e, quanto mais sabe, mais sofre.
Eclesiastes 1:18

Se a miséria dos pobres não é causada pelas leis da natureza, mas por nossas instituições, grande é nosso pecado.
Charles Darwin

O Bitcoin foi projetado para ser protegido da influência de líderes carismáticos.
Satoshi Nakamoto

***Caveats (advertência)*:** Nem um único conteúdo nesta obra é recomendação de investimento nem aconselhamento legal, nenhuma performance passada garante performance futura. Os coautores têm posições significativas de seu patrimônio nas nuvens. Bitcoin não é investimento, mas sim um *hedge* (proteção). Não existe investimento em ambiente de juro real negativo.

Maximalistas[1] consideram que: *shitcoins* como doge, shiba, bch e eth são ataques de engenharia social contra o Bitcoin; que mais de 90% dos *ICOs* são *scams* descarados; e, que se *DeFi* (finanças descentralizadas) é o futuro[2], provavelmente não será *onchain* — e sim em 2ª camada como *RSK*[3], *Liquid*[4] ou *Lightning*[5].

Altcoins foram úteis como alternativas para aumentar privacidade e escalabilidade de transações. Porém, não são mais necessárias para isso, elas podem ser úteis como *testnets* e como camadas de redundância para eventual falha na *mainnet*, mas a maioria das pessoas que tentam enriquecer ou “aumentar bitcoins” com *altcoins* acaba perdendo.

Ter valores depositados em corretora é risco de perda total, com falha na custódia; e, fazer *KYC*, informando seu nome, *e-mail* e endereço é risco de vida, de se tornar alvo de crimes ou perseguições totalitárias.

SUMÁRIO

PREFÁCIO
Só vamos sobreviver por causa do Bitcoin

Bitcoin Red Pill é o primeiro livro sério escrito em português sobre o Bitcoin. Diferentemente dos outros, é um livro que tenta dizer não só que é o Bitcoin, mas sim o porquê do Bitcoin. Não explica o Bitcoin somente como uma ferramenta, ou seja, qual sua função e mecanismo, mas mostra o Bitcoin como nossa única possibilidade de renascimento moral, material e tecnológico.

Este livro que não quer convencer ninguém. Você discorda que estamos em uma guerra de extermínio e que Bitcoin é uma das únicas armas à disposição do cidadão comum? Ótimo, faça o que você achar melhor para você e para sua família, siga sua vida como bem entender. Renato Amoedo e Alan Schramm só escreveram este livro porque estavam cansados de explicar várias vezes as mesmas coisas e, por interesse próprio, decidiram economizar tempo para tentar salvar o máximo de pessoas aptas. Infelizmente poucas pessoas neste mundo estão aptas a serem salvas. Se você se dispôs a ler este livro, muito provavelmente está entre elas.

Bitcoin Red Pill foi um livro escrito na era da internet para o indivíduo soberano. Como um manual de instruções, traz conceitos, teses, autores e dados que orientam o leitor a ir correr atrás das informações. A *internet* foi uma invenção magnífica pois diminuiu imensamente o custo da informação, mas é fácil se sentir desnorteado em sua galáxia. Bitcoin Red Pill mostra vários caminhos que podem depois ser trilhados pelo leitor interessado, seja este caminho sobre os aspectos técnicos sobre o Bitcoin, sobre a Escola Austríaca ou sobre colapsos civilizacionais.

Bitcoin tem pouco mais de uma década de existência. Um aspecto curioso de sua história é a quantidade imensa de pessoas com conhecimentos extremamente avançados de criptografia e programação que entenderam o Bitcoin só como “mais uma ferramenta”.

O que não falta é argumento de autoridade para confirmar essa impressão. O próprio Satoshi Nakamoto no *white paper* diz de forma muito sóbria que o Bitcoin é um “sistema de dinheiro eletrônico ponto-a-ponto”. Parece ser só mais uma mera ferramenta, não é mesmo? Sempre muito lacônico em suas correspondências, Satoshi confessou em um e-mail ser

melhor com *código* do que com palavras. Ainda bem: o Bitcoin funciona, isso basta.

No Bitcoin Red Pill, os autores buscam dizer o que Satoshi não diz: que tipo de sociedade humana o Bitcoin encontrou quando surgiu neste planeta e quais serão suas consequências mais profundas. Este é o primeiro livro brasileiro a navegar por nessas águas e traz um diagnóstico com o qual eu concordo integralmente: o Bitcoin encontrou uma natureza humana extremamente falha e encontrou também uma sociedade, a brasileira, repleta de golpistas, inflacionistas, malandros, *shitcoins* e pirâmides financeiras.

A escassez digital criada por Satoshi encontrou também um Estado completamente falido moral e financeiramente, que gasta mais que arrecada e joga a conta nas costas do povo por meio do roubo institucionalizado dos impostos e da inflação. O livro explica com detalhes as distorções de uma economia que gira com base em juros negativos e como funciona o Bitcoin, moeda forte e inconfiscável, num mundo de moedas estatais fracas e confiscáveis.

"Lembre-se de que a única coisa que ofereço é a verdade, nada mais", diz Morpheus. A pílula vermelha é a pílula mais difícil de engolir pois nos traz verdades que temos medo de admitir.

Renato Amoedo e Alan Schramm, além de trazerem relatos saborosos da história do Bitcoin no Brasil e de explicarem para o público leigo o funcionamento desta tecnologia e do mercado, foram corajosos o suficiente para oferecer este remédio amargo ao povo brasileiro.

Nesta segunda edição, lançada há menos de um ano da primeira, já vemos atualizações importantes devido à pandemia do vírus Sars-Cov-2. Os estragos desta pandemia criada em laboratório e da resposta ditatorial dos governos que fingem combatê-lo ainda não foram bem compreendidos amplamente. O que se sabe até agora não pegou o leitor da primeira edição Bitcoin Red Pill de surpresa: impressão massiva de dinheiro como nunca antes e propostas de controles de capitais ainda mais opressores por meio das assim chamadas moedas virtuais dos bancos centrais. A primeira edição saiu em setembro de 2020. Em julho de 2021 podemos dizer que as tendências apontadas pelo livro apenas se tornaram exponenciais.

Não há escapatória. Como dizem por aí, você pode não estar interessado na guerra, mas a guerra está interessada em você. Cada gráfico e cada linha

do livro é como um tapa na cara para acordar o brasileiro de um sono mortífero. Vai doer, mas valerá a pena.

— Guilherme Bandeira pesquisa e escreve sobre Bitcoin e sua regulação jurídica no Brasil. Foi tradutor do livro “O Padrão Bitcoin” para o português brasileiro e tem uma *newsletter* sobre o assunto https://guilhermebandeira.substack.com/publish

PRÓLOGO

Se quiser ir direto ao assunto, pule o prólogo - um roteiro com justificativas e análise contextual.

Certamente, o texto a seguir tem imprecisões, generalizações e erros, por isso não confie, verifique. Cada informação relevante tem referências em notas de rodapé ou no glossário. Temas mais complexos[6] vão ser objeto de volume posterior, *Bitcoin Black Pill - dinheiro, justiça e governo privados*.

Essa obra se dirige a facilitar a educação de pessoas dispostas a ser livres pela aquisição de fontes e conceitos para que viabilizem libertação pessoal e intelectual. “O início da sabedoria é chamar as coisas pelos seus devidos nomes”[7] – por isso se diz que “imposto é roubo”[8].

O livro foi escrito para economizar o tempo dos autores, que têm que explicar repetidamente a falsidade de diversos mitos. O Bitcoin (BTC). A cultura de criptografia e segurança digital é um bote salva-vidas para a liberdade e prosperidade de diversas famílias e uma das habilidades fundamentais para sobreviver financeiramente. Esse texto é um presente a quem quiser entender os motivos pelos quais:

1) Nos últimos 10 anos, não existiu nenhum produto financeiro de renda fixa (perda fixa) ou variável (perda variável, como as bolsas bolivarianas) com qualquer expectativa média de ganho real no *legacy*[9] (economia formal) – o que fica óbvio até mesmo pelo CDI e B3 (bolsa bolivariana do Brasil) perderem até do ouro guardado no colchão, sistematicamente, em ambiente de juros negativos e senhoriagem acelerada. Poupar em bitcoin é assumir alto risco, com alto potencial de ganho. Poupar em perda fixa ou perda variável é certeza de perda no longo prazo.

2) A maioria dos *traders* são viciados em apostas e as corretoras funcionam como cassinos. Não há como “viver de *trade*” sistematicamente – exceto se você tiver vantagem competitiva sobre os demais atores do mercado, seja na velocidade das execuções, vantagem na difusão ou acesso a dados ou notícias; ou vantagem na capacidade de manipular preço, o que não é o caso de ninguém que emprega dinheiro e tempo em cursos de *trade* vendidos no *YouTube*. A Literatura científica e lógica demonstra que, no longo prazo, mais de 95% das pessoas[10] se dão melhor empregando o tempo em seu trabalho (ou até mendigando), fazendo preço médio[11] e

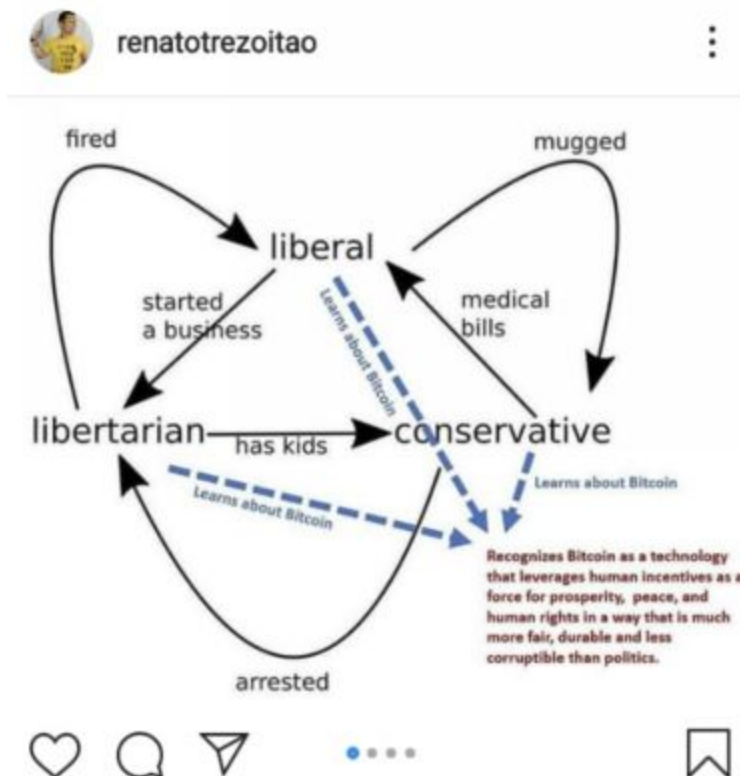
corrigindo a diversificação da carteira para manter proporção pré-determinada entre ativos, com rebalanceamento anual ou semestral. Só quem lucra sistematicamente nessa indústria são vendedores de cursos e relatórios e as corretoras, o resto é “catar moedas na linha do trem”[12].

3) Qualquer promessa de ganho sem esforço ou risco, como em “remuneração garantida acima do mercado”, é mentira: ou não há remuneração sistemática ou não é garantida[13]. As vítimas muitas vezes se enganam com o mantra “está pagando”. Ora, todos os esquemas *Ponzi* pagam enquanto entrarem mais recursos do que saírem. Não existe possibilidade de pessoas cumprirem perpetuamente rendimentos “garantidos” para fazer *trade* (que é realmente “ganhar de colher para perder de balde”) ou arbitragem (pior ainda, já que há deseconomia de escala em *slippage*[14]). Se você mandar bitcoins para um desconhecido, provavelmente não vai receber nada de volta – muito menos em dobro, como prometido nos golpes de *giveaway* (detalhados no capítulo II) com impersonificação de Elon Musk, Vitalik, Saylor e outras personalidades, como oferecido nesta live fake no Youtube.

4) Políticos, por mais bem-intencionados que sejam, não podem evitar o colapso e o totalitarismo por meios institucionais – como demonstrado por Olson, Hayek e Hoppe. Assim como os *déficits* sistemáticos e exponenciais dos Estados Sociais terminam, inevitavelmente, com a destruição de suas

moedas e de todos os ativos sob o alcance dos seus governos. "*Play stupid games, win stupid prizes.*"

5) Você só é dono dos bitcoins em endereços de que tem controle exclusivo das chaves privadas. Propriedade é um conceito absoluto. Se você tem saldo bancário (ou de ações ou até escritura de imóvel) e um burocrata pode revogar sua titularidade ou destruir seu valor com tributos (ou até regulações ambientais ou de zoneamento), então isso não é sua propriedade em seu conceito original, é outra categoria de direito. Ter saldo de bitcoins em corretora não é ter bitcoins (BTC). Assim como ter saldo de reais (moeda fiduciária) em empresa ou banco não é ter reais (é ter créditos que podem ser podres). Qualquer um pode criar endereços de Bitcoin em qualquer dispositivo, mesmo sem acesso à Internet. Qualquer um pode minerar, transacionar ou manter saldos em bitcoin sem autorização ou identificação. Ninguém controla o Bitcoin, nenhuma empresa, nem governo. O sistema não tem responsável nem chefe, não é possível impor sobre ele lei nacional ou decisão judicial, não há sequer quem citar em processos. Apenas empresas ou pessoas que operem com Bitcoin formalmente podem sofrer disciplina legal ou jurisdicional. "*Not your keys, not your coins*".

6) Os sinais de colapso civilizacional (dominância de valores femininos, *welfare*, diluição do valor da moeda, queda de fecundidade e de poupança, desestruturação de famílias etc.) são inevitáveis e cíclicos[15] (demonstrados por diversas teorias de ciclos intergeracionais, como a de Strauss-Howe ou de Sir John Glubb); e, em vez de se aborrecer com eles, é melhor aproveitar a crise como oportunidade e aceitar que Satoshi Nakamoto é John Galt[16].

7) O Bitcoin, se sobreviver por mais uma década, deve mudar o mundo mais do que a Internet já mudou – inviabilizando controles de capitais, expropriações e tributos involuntários, explodindo a erosão tributária, criando e destruindo mercados, e mudando brutalmente a hierarquia de valores. Quando o bitcoin desmonetizar ativos eles se tornam mais baratos: no caso do ouro, suas joias auríferas poderão ter mais peso pela metade do preço; com imóveis, você vai poder morar em um lugar muito melhor pela metade do custo; nos títulos e as ações, famílias vão voltar a ser remuneradas por poupança e poder viver de dividendos e juros reais. Já aconteceram e vão continuar a acontecer escândalos de manipulação de preço, ataques de spam, hacks em empresas, scams, proibições, ameaças de flippening com queda da dominância[17], criminalizações e restrições regulatórias e fraudes, mas “honey badger[18] don't care” (se o sistema continua rodando, o Bitcoin não se importa).

8) Moeda não é dinheiro. Em termos históricos, todas as moedas fiduciárias (*fiats*) emitidas por governos viraram pó ou tiveram a maior parte de seu valor perdido em termos reais (historicamente, em relação ao ouro). Assim como as coisas mais baratas da vida são pagas em moeda, as

demais são pagas com valores como sua liberdade, paz, saúde, amor, honra ou tempo de vida.

9) O maior investimento que se pode fazer é em educação real, que é, cada vez mais, oposta à instrução formal[19]. A verdade pode ser afirmada por critérios empíricos (como fatos históricos ou da realidade), ou por critérios lógicos (como a ética argumentativa *hoppeana*[20]), nunca por autoridade ou convenções[21] (como Direito Positivo[22]).

Red Pill vs Blue Pill

10) Os governos policialescos e totalitários travam uma guerra de extermínio contra a liberdade. Nessa guerra, as suas principais (embora não únicas) armas (para defender sua liberdade, patrimônio e modo de vida) são criptografia e descentralização. Se você não se prostrar à religião civil ponerológica, então, agora "o judeu é você" — seja hinduísta, *falun gong*, cristão[23] ou islâmico[24]. Todos os países serão infernos ou paraísos fiscais e regulatórios[25], não haverá meio termo, pode escolher:

Kim Jong Un warns that North Korea is running out of food as reports say a bunch of bananas now costs $45

Bill Bostock 11 hours ago

North Korean leader Kim Jong Un at a party meeting in Pyongyang, North Korea, in an undated photo released Wednesday by state media. KCNA via Reuters

ESTADOS UNIDOS MEJORA LA CALIFICACIÓN DE VIAJE PARA EL PAÍS

Miércoles

$0.25

Diario El Salvador

Loki llega hoy

ASAMBLEA APRUEBA LA LEY BITCOIN

La criptomoneda tendrá curso legal en el país. El BCR reafirma solidez del uso del dólar.

Países hermanos

LA FESFUT DEBE REGISTRARSE ANTE EL INDES ANTES DEL 30 DE SEPTIEMBRE

$245 MILLONES

DESTINADOS PARA CONSTRUIR EN LOS CHORROS EL VIADUCTO FRANCISCO MORAZÁN

ENCUESTA UTEC REVELA APOYO DEL 81.96 % AL REGRESO DE LAS CLASES SEMIPRESENCIALES

CON BOLETO A LA SEGUNDA RONDA

3-0

11) É relevante conhecer as dez operações básicas no ecossistema, seus prós, contras e quando e a quem são indicadas (*trade; hold; lend/margin trade; loan/*colateralizado; *scam; ransomware; bounty;* arbitragens*;* mineração e empreendedorismo).

Se já dominou os conceitos e ideias acima mencionados, não precisa continuar lendo.

Não se deve emitir opiniões públicas sobre assuntos técnicos para os quais não se tenha dedicado algumas milhares de horas em estudo ou experiência. Descobrimos o que realmente era o Bitcoin no início de 2015 e, após isso, temos dedicado a maior parte do tempo a compreender e interagir com o ecossistema.

Aprendendo com os erros dos outros, evita-se o prejuízo. Da mesma maneira que dependemos de tutores no início da nossa jornada, temos o dever de facilitar o caminho dos que vêm depois, fazendo nossa parte como a "*pleb*" do neofeudalismo de Max Keiser, que logo será a nova nobreza natural, após cumprir a missão como "*cyber hornets*"[26].

Mises Capital vs Samy Dana[27]

Michael Saylor
@michael_saylor
#Bitcoin is a swarm of cyber hornets serving the goddess of wisdom, feeding on the fire of truth, exponentially growing ever smarter, faster, and stronger behind a wall of encrypted energy.
Traduzir Tweet
3:51 PM · 18 de set de 2020 · Twitter Web App
4.009 Retweets 725 Tweets com comentário 20 mil Curtidas
Eiran Simis @eiransi... · 09 dez 18
A quantidade de Bitcoin é conhecida, já a de ouro ninguém sabe ao certo. Mas na dúvida é bom ter os dois.
1 8
Henrique Bredda
@hbredda
Em resposta a @eiransimis @Vinicius1_Bsb e @JamesGRickards
Bitcoin?! Pra q complicar? Sai dessa.
21:46 · 09 dez 18 · Twitter for Android

É uma honra viver esse momento da história, em que dezenas de paralelos dos colapsos civilizacionais se repetem, tais como: queda de fecundidade, efeminação[28] e infantilização de pautas públicas, diluição da moeda, *welfare* deficitário, desestruturação de famílias, corrupção e ampla captura administrativa. O Bitcoin é uma das tecnologias para servir de “bote salva-vidas” para quem perceber a realidade, por isso se diz que “cada um compra (e vende) o bitcoin no preço que merece” ou “quem não comprar bitcoins sorrindo, vai comprar satoshis chorando”.

Se você é capaz de ler com boa velocidade e aproveitamento em inglês, então, para aprofundar, leia *The Internet of Money 1,2 e 3*, do Andreas Antonopoulos, e, se for programador, o *Mastering Bitcoin*, do mesmo autor, ou *Programming Bitcoin: Learn How to Program Bitcoin from Scratch*, de Jimmy Song. Um manual passo a passo é o *21 Lessons: What I've Learned from Falling Down the Bitcoin Rabbit Hole.*

O *opus magnum* em português é *O Padrão Bitcoin*, de Saifedean Ammous.

Esses livros são superiores, em muitos aspectos, a qualquer outra coisa e são facilmente encontrados, gratuitamente, na Internet. A leitura do verbete *Bitcoin*[29] na Wikipédia (em PT e EN) ou Bitcoin WiKi[30] (EN) também são excelentes como primeiros passos.

Sobre as implicações políticas e sociais do Bitcoin, recomenda-se *Bitcoin Revolution: Ending Tyranny For Fun & Profit*[31].

Se você não sabe quem é Menger, Bawerk, Mises, Hayek, Rothbard, Hoppe e os Friedmans (os três), é altamente recomendado que busque suas obras seminais – igualmente disponíveis em português em diversos PDFs gratuitos na Internet nos sites dos Institutos Mises Brasil[32] e Rothbard Brasil[33].

Não precisa ser libertário para ser *bitcoiner*. Diversas figuras no país e no exterior (como o próprio Andreas Antonopoulos) têm tendências "esquerdopatas" claras. Porém, se não compreender os autores acima mencionados, não entenderá os conceitos de lastro, moeda fiduciária (*fiat*), dinheiro, senhoriagem, reserva fracionária, ciclos econômicos e as reais consequências da guerra ao dinheiro e dos juros negativos.

Sem compreender a Escola Austríaca, não entenderá em sua totalidade conceitos como: captura administrativa, Lei de Gresham, Lei de Wagner, Lei de Michels, Curva de Laffer, Efeito Cantillon; fatores estruturais deflacionários (demografia/envelhecimento, desalavancagem bancária, disrupção tecnológica); a insustentabilidade dos níveis de endividamento máximos, públicos e privados; a velocidade da moeda; e, a diferença entre inflação, base e agregados monetários[34] e os índices de preços.

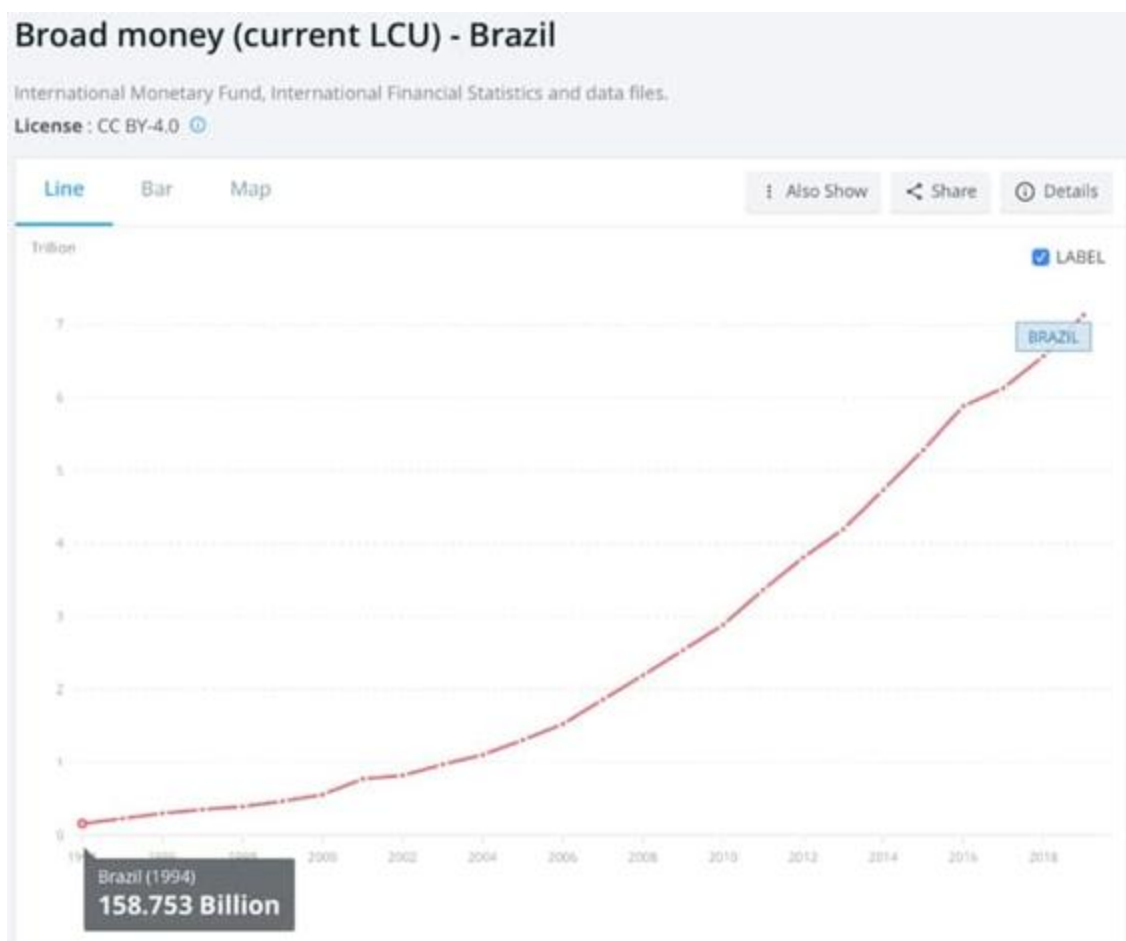
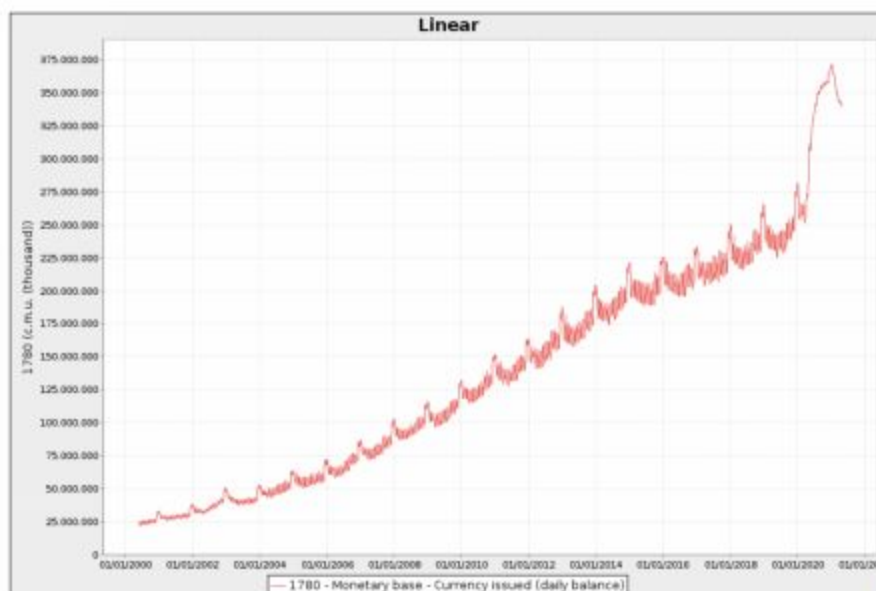
O entendimento da realidade, lógica ou empírica, é a educação real.

É devido a esses fatores deflacionários que o governo conseguiu aumentar os agregados monetários (base monetária e dívida pública) por mais de 10 anos em mais de 10% ao ano (em média) e ainda manter alegações de que remunerações patéticas de um dígito são “juro real

positivo”. A vovó *nocoiner* recebe 90% do CDI (menos de 5%aa), tem mais de 15% de perda real (devido a inflação) e ainda tem que pagar imposto de renda.

Quando você compreende que o mundo – e o Brasil – vivem em um ambiente de juro real negativo (descontado o aumento da base monetária e o risco), entende que nenhum produto financeiro convencional pode ser considerado investimento. Aí, sim, é possível entender por que produtos como ouro[35] (que sequer pode ser considerado investimento) ganharam da inflação oficial e até mesmo do aumento do salário mínimo desde o início do Plano Real.

Hipoteticamente, se a economia no país crescesse, em média, 1% ao ano na década e o total de meio circulante aumentasse em mais de 20% a.a., o governo enriqueceria, diretamente, em 19% ao ano devido à nova moeda criada; e, indiretamente, através do aumento de impostos decorrente.

Como é demonstrado nos gráficos, a realidade é pior que isso[36]:

Segundo o Banco Central do Brasil[37]: "A base monetária alcançou R$427,8 bilhões em outubro, aumento de 4,7% no mês e de 46,3% em doze meses” (gráfico abaixo, também do BCB, não cobre período recente)[38]. Ora, se o PIB caiu e o número de reais aumentou em mais de 46% em 2020, quanto foi a perda de quem poupou em reais, mesmo que remunerado pela SELIC (abaixo de 3% em 2020)?

No resto do mundo, a situação não é muito melhor, os agregados monetários globais (moedas de todos governos) cresceram em um ano (até meados de 2021) mais de 32% do PIB global e os mercados comemoram um crescimento estimado em 6% a.a. (medido nessas moedas diluídas em 32%, resulta em perda real de 26%).

Há três formas principais de governos se financiarem: a) tributos (limitados pela curva de Laffer); b) emissão de moeda (limitada a destruição de valor do meio circulante, como na Venezuela e no Zimbábue); e, c) emissão de dívida (limitada a disposição de credores a emprestar). As três fontes estão próximas dos limites.

As consequências de aumentar a carga tributária são: 1) o aumento dos custos de produtos e serviços e a destruição de riqueza devido às transações que deixam de ser realizadas por essa subida de preços (perda do bem-estar social); 2) enriquecimento de “aspones” e empobrecimento de produtores e consumidores; e, 3) decomposição de instituições, com ampliação das vantagens de comportamentos oportunistas.

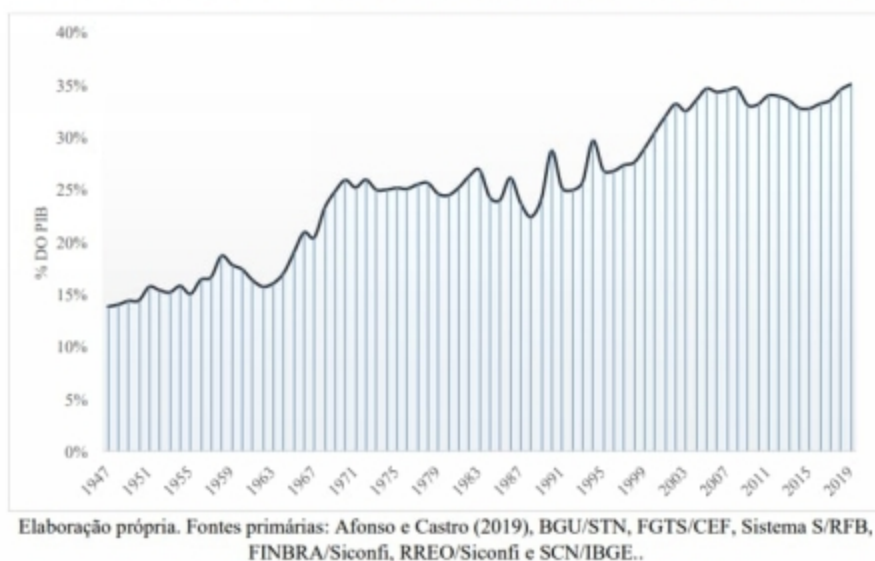
Se um banco central emite mais moeda, ele dilui o valor daquelas já existentes (inclusive o valor de sua própria dívida em moeda soberana), e destrói a riqueza de quem poupou em *fiat*, traindo e empobrecendo quem confiou nele.

Quando o governo emite dívida, ele retira investimentos que iriam para atividades produtivas, e destrói todos os empreendimentos com expectativa de retorno corrigida pelo risco, inferior à remuneração de seus títulos.

Também no gasto dos recursos arrecadados, o Estado destrói riqueza, uma vez que seus gastos não respeitam critérios de mercado e competem com os entes que realmente geram riqueza, e eleva para esses o custo dos bens e serviços que venham a adquirir. O "monopólio da violência" é uma máquina de produzir corrupção, miséria e terror.

Você realmente acha que há alguma chance de as curvas de carga tributária e *déficit* serem invertidas? Como proteger sua família disso?

Gráfico 1 - Evolução Histórica da Carga Tributária Bruta no Brasil- 1947/2019

Elaboração própria. Fontes primárias: Afonso e Castro (2019), BGU/STN, FGTS/CEF, Sistema S/RFB, FINBRA/Siconfi, RREO/Siconfi e SCN/IBGE..

Com dados mais atualizados, seria ainda mais brutal a demonstração dos *déficits* públicos, carga tributária, aumento dos agregados e endividamentos estruturais.

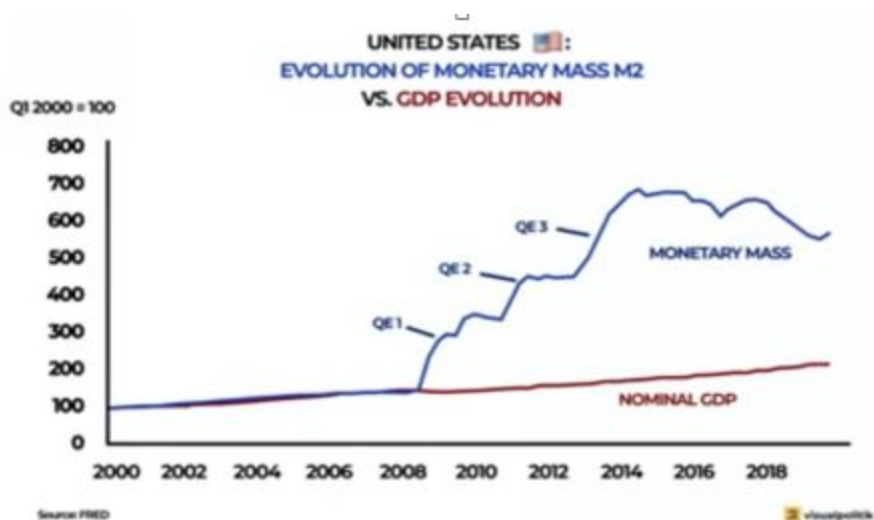
Se você investiu em qualquer coisa que não rendeu líquido e descontado de risco mais de 46,3% em 2020 em reais, perdeu riqueza, era melhor ter estocado bem não perecível ou comprado galinhas. A única medida objetiva de inflação é o aumento da base monetária, que foi superior a 20% a.a. em Real (R$ ou BRL) nos últimos anos (somando reais criados por meio das reservas fracionárias dos bancos e pelo governo).

Esses efeitos não são percebidos por muitos, devido aos fatores estruturais de redução de preços, porém, suas consequências em longo prazo são inexoráveis – uma vez que os fatores deflacionários não são perpétuos. Quem não perceber, vai sofrer. O Brasil envelhece 6,5x mais

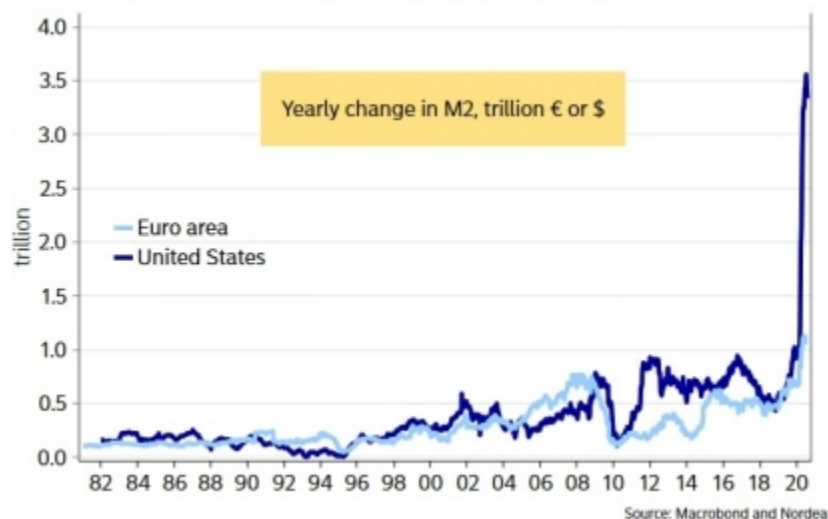
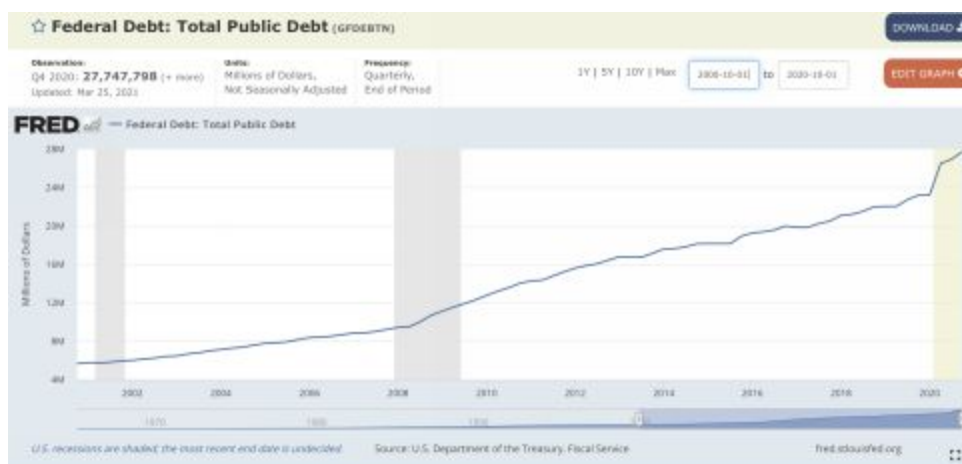
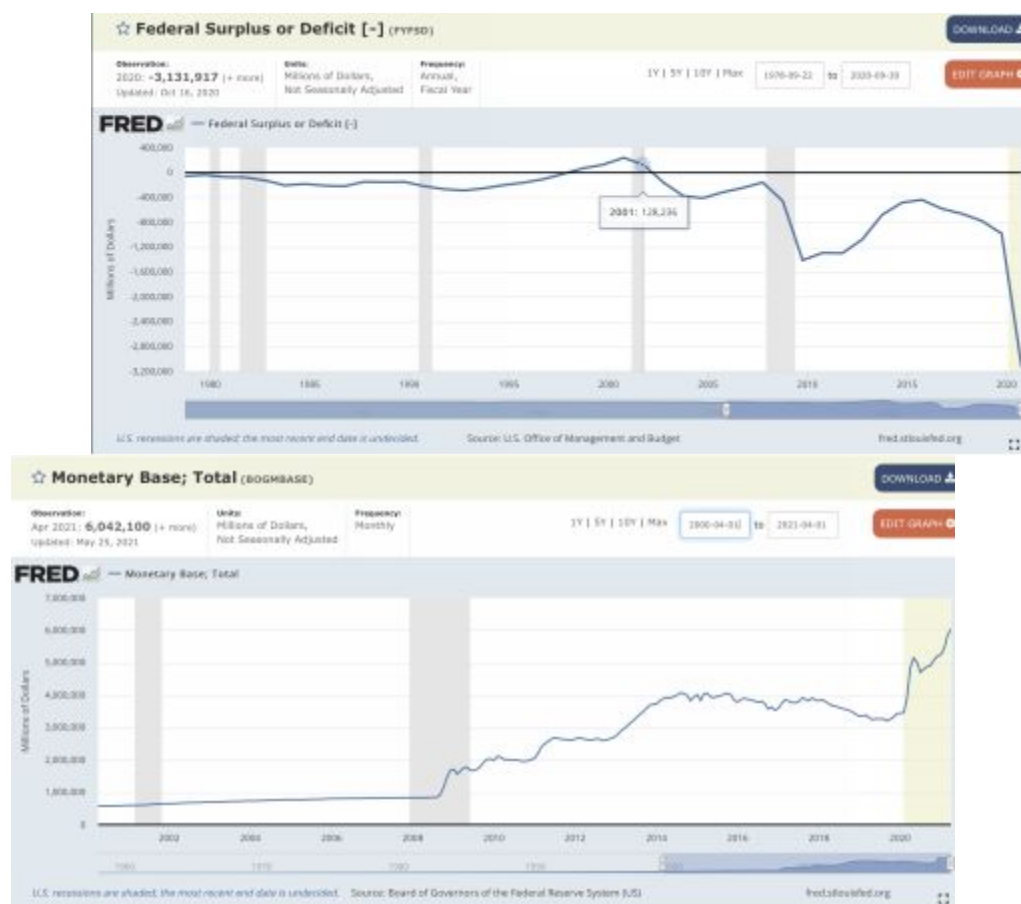
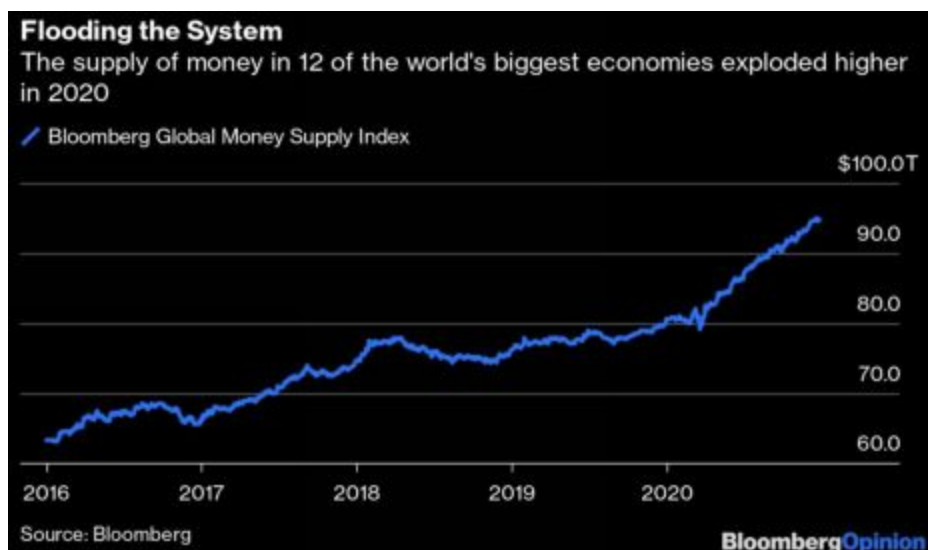
rápido que os Estados Unidos e o dividendo demográfico já foi desperdiçado.

O imposto inflacionário (*hidden tax* de Friedman) não apenas dilui o valor dos reais (moeda fiduciária), como aumenta o pagamento de impostos de renda, via aumento do valor nominal dos bens e dos salários[39]. Ora, se um bem (seja casa, carro, ação ou barra de ouro) que custava 100 reais é vendido 30 anos depois por 100 mil reais, formalmente, 99,9% do seu valor de venda seria "lucro" para fins tributários, mesmo que seu valor real 30 anos depois fosse inferior ao seu valor real original. Exemplo claro é o grama de ouro: sua cotação em julho de 1994 foi R$ 11,45; se vendido em maio de 2020, quando a cotação chegou a R$ 321,35, formalmente, 310 reais seriam "lucro" e tributáveis, mesmo que esses 310 comprassem menos bens em 2020 do que 11,45 compravam em 1994.

Ou seja, o imposto inflacionário aumenta a arrecadação ao inflar nominalmente a renda; amplia a capacidade do Estado de se endividar ao reduzir o valor real de sua dívida; dilui o valor dos detentores de moeda e títulos de dívida, empobrecendo quem confiou no governo; e subtrai das famílias os benefícios deflacionários da tecnologia. Por isso, a inflação deve ser medida por aumento da base monetária e não por índices de preços, como IPCA, no Brasil, ou CPI, nos EUA, (usualmente manipulados).

Grandes mentes discutem ideias, mentes medianas discutem eventos, e as mentes pequenas discutem pessoas.

"A study by Hirschman Capital shows that out of 51 cases of govt debt breaking above 130% of GDP since 1800, 50 governments have defaulted. The only exception, so far, is Japan. We mention this because the IMF expects US Debt to hit 141% by the end of 2020."

Felix Zulauf

11:03 · 23 Aug 20 · Twitter for iPhone

Embora no *whitepaper*[40] original Satoshi não tenha feito qualquer consideração explícita sobre política ou economia, a mensagem incluída no Bloco Gênese[41] do Bitcoin e as postagens em fóruns[42] do seu criador, Satoshi Nakamoto, deixam claro que o Bitcoin só se tornou necessário devido aos abusos dos governos em emitir moeda desenfreadamente (até agora o número de reais criados pelo governo aumentou mais de 45x nominalmente e mais que triplicou, em relação ao PIB, desde 1994) e em manter níveis exponenciais de *déficit*, vide o governo norte americano, que gasta mais do que arrecada desde 2001[43]:

O resultado disso é a explosão na base monetária do dólar, em mais de 10x, e da dívida pública, em mais de 5x, nos últimos 20 anos:

Moeda puramente fiduciária (*fiat*) é a que não é conversível e só é aceita por imposição legal, denominada “curso forçado”[44], como o real ou o euro. O poder de emissão ilimitado cria estímulos perversos para que *déficit* e endividamento exponenciais sejam uma constante e atinjam níveis sem precedentes. Há 10x mais riqueza em *fiat* que em ouro[45]:

As políticas de guerra ao dinheiro (restrição de uso e propriedade de moeda alodial[46]) e os juros negativos permitem ampliar ainda mais o endividamento público e o totalitarismo financeiro.

Exemplos dessas limitações ao uso e à propriedade da moeda física, ouro e outras formas de moeda alodial são, desde 2015[47], as restrições de uso de moeda para transações privadas na Itália, na França e na Espanha (coroadas com a retirada de circulação das cédulas de 500 euros[48]); e a propriedade limitada sobre ouro na Alemanha e na Índia, e proibida nos Estados Unidos de 1934 a 1975[49].

O resultado do juro real negativo, além da elevação artificial dos valores dos ativos, foi a desigualdade social sem precedentes. O juro mundialmente apresentava tendência de queda desde 1981, mas o ápice do processo foi demonstrado na última década, em que até ouro[50] no colchão superou métricas como o índice Bovespa ou o CDI (ou seja, qualquer investimento bancário sem riscos extremos) – o que tende a se agravar com a normalização dos juros e destruição de valor dos ativos convencionais (*legacy system*).

Como demonstrado nas fórmulas do valor presente líquido e do *CAPM*[51]. (considerando riscos de mercado e idiossincráticos), os ativos que têm fluxos de caixa independentes de taxas de juros (como ações, pontos comerciais e imóveis para aluguel) são usualmente avaliados pelas expectativas médias de fluxos descontadas das taxas de juro. Ou seja, considerando os riscos na expectativa média de retorno, um ativo qualquer que gere renda teria a sua avaliação equivalente ao quanto de moeda no sistema bancário pagaria no juro de mercado; quanto menor a taxa de juro, maiores ficam as avaliações dos ativos, *Ceteris Paribus* (considerando demais fatores constantes).

Nesta simplificação, se uma casa gera aluguel de R$ 1.000 por mês independente de taxa de juro e a taxa é de 1% ao mês (12,68% ao ano), a casa valeria R$ 100.000, pois 1.000 é 1% de 100.000. Se a taxa de juro cai para 0.1% ao mês, agora ela gera fluxo equivalente a R$ 1.000.000, pois 1.000 é 0.1% de 1 milhão; e, se o juro cai para 0.1% a.a, são necessários mais de R$ 12.000.000 (doze milhões) em investimentos para equivaler a seu aluguel.

Imagine agora o tamanho da distorção (e de como estão inflados os preços de imóveis e ações) quando os juros reais (descontados da inflação) são negativos e o quanto os ativos podem se desvalorizar quando os juros voltarem ao normal. Este também é o motivo de haver enorme potencial de desvalorização dos ativos com a normalização de juros.

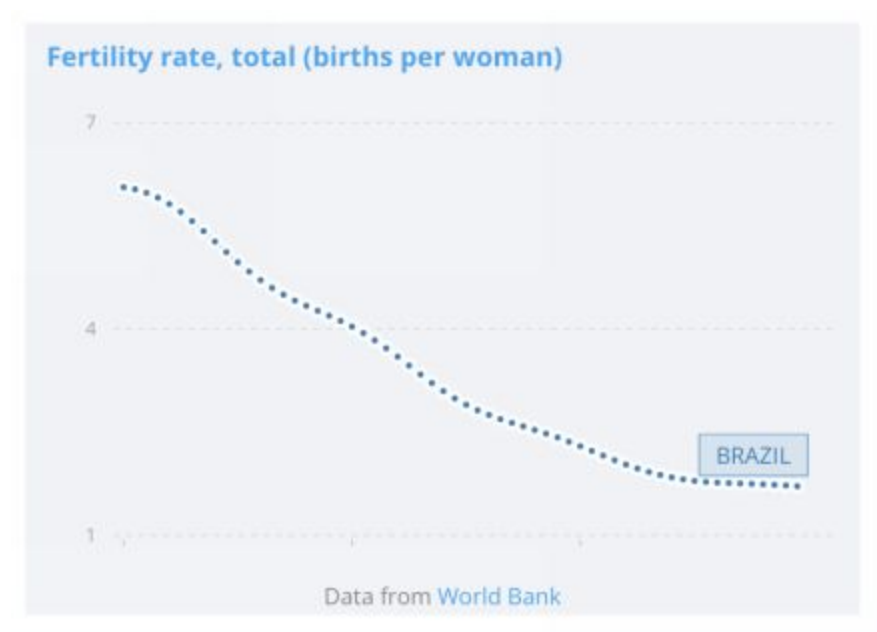
Além da captura administrativa[52], esse tabelamento imoral de preço foi a principal causa do aumento das desigualdades sociais no mundo, nas últimas décadas. Primeiro, multiplicando em ordens de grandeza a avaliação dos ativos dos "ricos" (às vezes apenas sua residência, que em muitos centros urbanos multiplicou centenas de vezes de valor nominal em gerações); e, segundo, desestimulando a poupança (facilitando endividamento subsidiado, com hipotecas, como bem descrito no filme *The Big Short).* Por isso, os bilionários multiplicaram suas fortunas, enquanto os micro e pequenos empresários foram obliterados no caos social[53] decorrente do vírus chinês, no que se denominou "recuperação em K" - *wall street* para cima, *main street* para baixo[54] (privilegiados, cantilionários para cima e empreendedor honesto das classes média ou baixa, destruído).

Além da destruição de valor derivada da normalização dos juros, outros dois fatores vão corroborar a perda de valor dos ativos convencionais (imóveis, ações e títulos): primeiro, a reação agressiva dos governos

(sistematicamente deficitários) em face das quedas na arrecadação (erosão tributária, elevação dos níveis de regulação e tributação); e, segundo, as mudanças tecnológicas, que tornam grande parte (se não a maioria) dos imóveis, ações e moedas obsoletos. Teletrabalho e comércio virtual reduzem a demanda por imóveis comerciais, como grande exemplo dessa tendência[55].

Assim, quem conta com investimentos em imóveis, ações ou títulos pode ter seu futuro comprometido como aqueles que contavam com aluguel de linhas telefônicas, placas de táxi ou dividendos da *Kodak*.

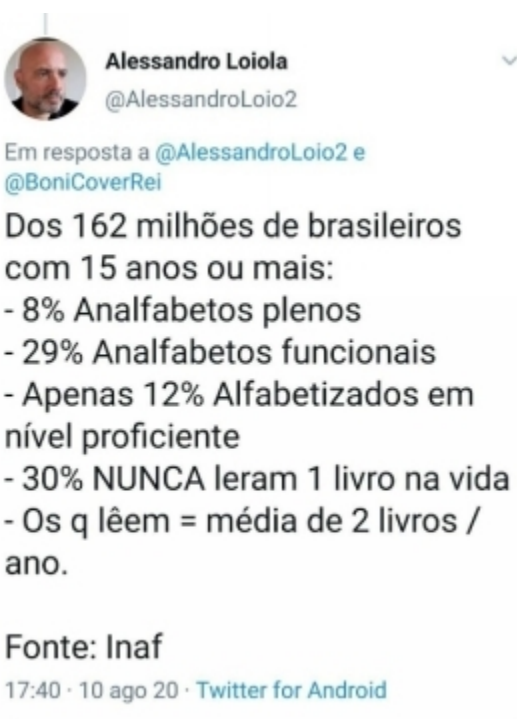
Quem conta com previdências privadas ou públicas não está em melhor situação. As previdências por capitalização são inviáveis em regime de juro real negativo (investimentos perdem sistematicamente valor, inclusive com taxas de administração) e as previdências por sistemas de caixa (repartição) são matematicamente inviáveis com taxas de fecundidade (e taxas de emprego e contribuição) insuficientes e decrescentes (fecundidade no Brasil cai desde 1950, já está abaixo de 1,7 e seria necessário estar acima de 2,2 para manter a população estável).

A população brasileira já envelhece exponencialmente desde 2018 e, com o fim do dividendo demográfico[56], tende a cair após 2030-2040[57], até que as motivações para ter famílias numerosas voltem a existir:

A infância mental[58] é denotada pelas decisões e reações emocionais em vez de racionais, pela efeminação da sociedade[59] e pela incapacidade de assumir responsabilidades básicas, atribuindo a outras pessoas ou instituições a obrigação de resolver seus problemas pessoais e a culpa pelas suas derrotas, como se observa nos eternos adolescentes que acreditam que "o Estado tem dever de dar educação e saúde gratuitas"; ou aqueles que, sem trabalhar, "estudam para concurso" ou fazem a terceira ou quarta graduação aos 30 (como Charlinho do Hermes e Renato, educacionistas); ou aqueles fracassados que culpam sombras pelo sua derrota – terceirização moral –, seja a sua cor, os judeus, o "capitalismo opressor" ou os seus pais. Quando alguém entende que "ninguém te deve nada", torna-se adulto mentalmente.

Se optar por tomar a *Matrix red pill* e ser livre, vai passar a ser responsável – vai ter que estudar, entender e assumir as consequências de seus atos. Liberdade absoluta é responsabilidade absoluta.

Ser livre não é sinônimo de fazer o que tiver vontade. Quanto mais autodisciplina e autocontrole, quanto mais entendimento, mais liberdade, mais poder e mais responsabilidade. Então, se está pronto para deixar a infância política, mental e financeira, pode continuar.

Já está mais que consolidado que a instrução formal hoje é oposta à educação real – como já demonstraram Taleb e Robert Kiyosaki no livro *Fake money, fake teachers and fake assets* (Ativos, moedas e professores de mentira). Bill Gates e Zuckerberg largaram os estudos para empreender, Amancio Ortega e Steve Jobs nunca foram alunos de qualquer faculdade e Thomas Edison largou a escola no segundo mês. Isso sem contar os exemplos de sucesso sem formação universitária no país, desde Luís Inácio e Alcolumbre até os bilionários Joesley e Wesley Batista – que sequer terminaram o colegial.

Testes oficiais, como ENEM e ENADE, indicam que a maioria dos universitários no país são analfabetos em algum grau.

No passado, o consenso era o pensamento mítico e mágico e abordagens concretas e objetivas eram minoritárias: alquimia era dominante e química estudo marginal; astrologia foi dominante por séculos e astronomia era marginal.

Hoje, com a academia profundamente infiltrada e subvertida[60], disciplinas inteiras continuam dominadas por pseudociência, misticismo e ideologia pura, como a Nutrição baseada em Ancel Keys[61], a Economia baseada em marxistas e keynesianos, ou o Direito baseado em Direito Positivo – refutado desde seu início – ou em ativismos ainda mais baixos (intelectual e moralmente).

Políticos têm interesse que as crianças do povo sejam educadas para serem independentes, ricas e inteligentes, ou dependentes, pobres e imbecilizadas?

Quando alguém compreende a resposta desta pergunta, entende que o governo/socialismo/comunismo não é incompetente. Ao contrário, o governo é ALTAMENTE eficiente em aumentar o poder do Estado e a riqueza dos governantes – incluindo aí todo estamento burocrático: os eleitos, o *deep state*, os "aspones" concursados e, especialmente, os "amigos do rei" ou "consórcio"[62], como prefere Olavo de Carvalho em *Os EUA e a Nova Ordem Mundial*, ao se referir aos maiores beneficiários da "captura administrativa", degeneração derivada do aumento do Estado além de suas funções próprias de jurisdição e defesa.

Olavo de Carvalho[63] atingiu seu nível de popularidade e influência exatamente por despertar na população o entendimento de que: 1) o coletivismo é expressão do mal absoluto (em termos de direitos naturais ou até espirituais) – trazendo a público fontes como Eric Voegelin[64], Lyle Rossiter (Mentalidade Esquerdista), Lobaczewski (Ponerologia Política) e Solzhenitsyn (Arquipélago Gulag); 2) o Estado tende a aumentar seu poder exponencialmente, como descrito no *Jardim das Aflições*, apenas com argumentos retóricos e históricos, como os de Jouvenel (*O Poder: história natural do seu crescimento*); e 3) o meio de aumentar os poderes do Estado de maneira exponencial é a engenharia social, planejada e insidiosa, destruindo a inteligência pela instrução formal controlada por burocratas, desestruturando as famílias com leis feministas e estímulo à promiscuidade, infiltrando e subvertendo instituições sociais (incluindo aí a moeda),

infantilizando eleitores e efeminando homens (corrupção da inteligência)[65].

Os problemas do Professor Olavo[66] com os pagamentos do seu curso são excelentes exemplos da urgência da educação em relação a criptomoedas. Se o curso fosse pago em bitcoin, ou outra cripto pseudo-anônima, nem que fosse *stable dollar*, problemas com o *Paypal*, PagSeguro e *IRS (Internal Revenue Service)* ou RFB (Receita Federal do Brasil) seriam evitados – e a identidade dos alunos preservada, em vez de exposta a governos e corporações militantes para expurgos presentes e futuros.

Assim como a educação pública não visa educar, a imprensa progressista não tem como objetivo informar nem convencer. Ela tem como objetivo intimidar, amedrontar e dessensibilizar as vítimas (subversão e contrainteligência). **A maior parte das concessões públicas visa abertamente à desinformação, à inversão de valores morais e às "*fake news*", como popularizado por Trump.**

A infância política é identificada pelo cultivo da "Arrogância fatal"[67], crença irracional de que a sociedade pode ser planejada e regulada positivamente por uma autoridade central sem qualquer *"skin in the game"*[68], devidamente refutada por Hayek, dentre outros, no *"O uso do conhecimento na sociedade".*

A infância financeira[69] advém da crença de que é possível constituir riqueza – ou mesmo manter padrão de vida – pagando metade de sua renda de tributos e usando a outra metade para pagar por aquilo que já pagou ao Estado para te prover. Essa condição de infância é usualmente evidente em quem usa moeda estatal exponencialmente diluída para acumular sua poupança na "perda fixa"; para quem confia em contribuições a sistemas de previdência insustentáveis; ou para os "arrojados" que confiam o futuro de suas famílias exclusivamente na compra de ações de empresas e fundos submetidos à soberania de Estados Sociais. Se quiser entender melhor que dinheiro é a forma de concentrar TEMPO e LIBERDADE, assista no *YouTube* a *Hidden secrets of money*[70], com Mike Maloney.

Se o leitor tiver menos de 40 anos, provavelmente não vai receber nada significativo de aposentadoria, mesmo que seja servidor público. Caia na real: de onde acha que o governo brasileiro vai tirar dinheiro para pagar aposentadoria em 35 anos quando for o país mais velho das Américas? Sua poupança e sua eventual herança em 10 anos poderão não valer nada, como os ativos dos venezuelanos, que viraram pó. A solução está no

conhecimento. Se continuar a leitura, vai ser exposto a verdades que podem te libertar.

Por esses motivos, foi criada uma alternativa de reserva de valor superior ao ouro em certos critérios aristotélicos do DINHEIRO: o Bitcoin. Os atributos de moeda são fungibilidade (as unidades serem indistinguíveis umas das outras), divisibilidade, durabilidade, transportabilidade e, se além de moeda for dinheiro, deve ter o atributo da escassez (para servir de reserva de valor). O bitcoin é mais divisível, mais transportável, mais fungível; já é mais escasso em oferta marginal (inflação anual) que o ouro após maio de 2020; e até agora tem sido durável, embora nesse critério o *track record* do ouro imponha superioridade com milhares de anos e maior resiliência.

Pontas de flecha, contas (para fazer pulseiras e colares) e ferramentas de obsidiana (rocha magmática) foram demonetizadas pelo cobre. O cobre foi demonetizado pela prata. A prata, pelo ouro. O ouro, por *fiats*. Agora, *fiats* estão sendo demonetizadas pelo Bitcoin, a abstração suprema. Esse processo ocorreu no mundo em milênios — e no Brasil em poucos séculos com os indígenas, denotando ser orgânico[71].

Em todos os processos anteriores, os “amigos do rei” enriqueceram às custas dos poupadores. Agora, o varejo (a *pleb*, pequeno investidor) enriqueceu antes do *legacy* (instituições tradicionais, fundos, bancos e governos). Por isso, Bitcoin não é a oportunidade da geração, mas a oportunidade da história da humanidade.[72]

Há falha grave na argumentação de quem defende que a morte das moedas fiduciárias, o fim das empresas zumbis e a irrelevância de governos

são processos inevitáveis devido à queda dos custos de transação e aumento dos custos administrativos (como detalhado por Coase[73] e Calabresi/Melamed[74]). Quem prevê a inevitabilidade do futuro baseado em projeções de tendências econômicas são os marxistas e malthusianos – ambos erram completamente. Neste aspecto, há mais razão com o Paulo Kogos do que com Peter Turguniev.

A engenharia social da “fraudemia” deixa claro como populações podem aceitar a destruição de grande parte da economia privada e a revogação de liberdades com base em mera propaganda estatal ou atos abertamente ilegais.[75]

Há pessoas muito inteligentes que não entendem a urgência e utilidade do Bitcoin, simplesmente por viver em bolhas de crença na legalidade e legitimidade estatal. Se você acredita que o governo te deu educação, saúde e segurança – e que a moeda emitida por ele te protege de perdas – não haveria porque migrar para as nuvens. Classe média do primeiro mundo, aspones, marajás, empresários amigos do rei e os mais corrompidos moralmente vão ser os últimos a aceitar[76]. Por isso que se diz que o Bitcoin é um buraco negro que atrai primeiro aqueles elementos de maior massa e densidade, intelectual e moral[77].

Procedimentos de *lockdown*[78] (confinamento de gente inocente e saudável) sem qualquer fundamento empírico ou lógico (que destroem empresas, empregos e poupança) ou a obrigatoriedade de uso de máscaras de pano ineptas e insalubres[79], mesmo após resultados superiores (em instituições, economia e imunidade de manada) em países que não adotaram o *lockdown*, como Suécia e Uruguai, demonstram como a humanidade pode perder liberdades e riqueza rapidamente e sem motivo real, vez que a mortalidade da doença é de menos de 2% em septuagenários (*Diamond Princess*)[80] e de menos de 1:1200 em saudáveis (*USS Theodore Roosevelt*)[81], sem tratamentos específicos.

Trata-se de arrogância fatal prever o resultado de futuras interações de mercado entre bilhões de agentes. Como experiências de ditaduras totalitárias na China, Cuba e Coreia do Norte provam, governos podem, sim, interferir em custos de transação, e novas tecnologias podem reduzir brutalmente os custos administrativos e de controle social. Várias tecnologias superiores em diversos aspectos já foram rejeitadas no teste real de eficiência no mercado — ou por interferência regulatória.

Essa argumentação indica que a *web* 1.0 (sites estáticos e não interativos) foi capaz de tornar serviços postais obsoletos com os *e-mails*, locadoras de DVDs e venda de CDs igualmente eliminados por serviços de *download*; a *web* 2.0 (*sites* interativos e *apps*) destruiu grande parte dos mercados de transportes e táxis (*Uber* e similares), telefonia (*Skype*, *WhatsApp*...), comércio presencial (com entregas como *Rappi*, *Uber Eats* e *iFood*) e até de imóveis comerciais (com telemedicina, teletrabalho e escritórios virtuais); e a *web* 3.0 (inteligente e descentralizada) iria igualmente inviabilizar a capacidade de governos de proibir ou interromper a oferta de serviços e produtos pela Internet, vez que o Uber pode ser fechado ou interrompido em uma jurisdição, mas não o Bitcoin e o *Arcade City*[82].

Com a substituição de *smartphones* por *wearables* (dispositivos vestíveis), é possível que o governo veja e ouça mais do que as pessoas veem e ouvem em seu meio (com câmeras nos óculos de realidade aumentada ou virtual – *AR/VR*). Com a popularização do uso da Internet, *Big Data* e *Machine Learning*, grandes empresas têm poder de interferir na opinião pública e eleições (como no escândalo da Cambridge Analítica e nos diversos escândalos que comprovaram que *Facebook*, *Google*[83] e outras empresas têm compromissos íntimos com grupos de extrema-esquerda[84]).

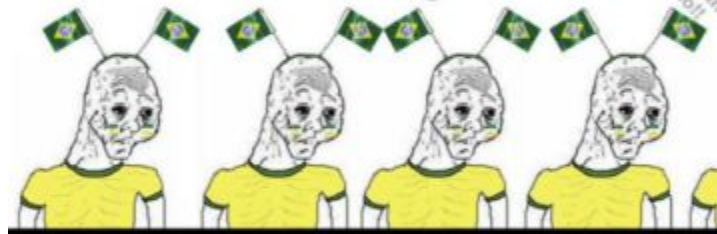
Com o fim das moedas alodiais, novos níveis de totalitarismo e controle são iminentes[85] – inclusive, permitindo juros ainda mais negativos e mais gasto estatal. Se o mundo futuro será um paraíso regulatório e fiscal comparado com o presente, ou se será um inferno totalitário, depende das ações que tomarmos hoje – inclusive, por meio da divulgação do Bitcoin e do desinvestimento do *legacy*. Essa foi a maior motivação para escrever esta obra.

Pouco ou nada importam as boas intenções de qualquer governante. Como se diz no ditado popular: “de boas intenções o inferno está cheio”[86]. Como já foi comprovado por Hayek em *O caminho da servidão*[87], uma vez adotado o Estado Social (*Welfare*), o caminho para o colapso é inevitável.

Para terminar o prólogo, é necessária a demonstração (corolário) do quão frágil e improvável qualquer melhora pelo voto, em uma breve digressão sobre o governo que seria oposição a tudo que estava posto até então:

Miguel Nagib
June 19 at 3:09 PM ·

IMPOSTOR E TRAIDOR
Bolsonaro não só não cumpriu a promessa de livrar as escolas da doutrinação e da ideologia de gênero, como boicotou a única iniciativa da sociedade que combatia essas práticas, e agora, para completar a traição, sancionou uma lei que oficializa a engenharia social feminista em todas as escolas brasileiras.

65 · 11 Comments 8 Shares

Bolsonaro foi eleito com as principais promessas de combater o desarmamento e o comunismo, desaparelhar a Administração e reduzir o Estado. Após eleito foi usualmente referido como “bonobo”, “broxa”[88] e “maior traidor e covarde dos 500 anos" por diversas personalidades que apoiaram e financiaram sua eleição, por não ter desnazificado[89] a Administração, permitindo a explosão da corrupção[90], desmoralização, emissão de moeda e dívida e até mesmo a queda de produção e consumo de energia anos seguidos[91], com "fuga de cérebros sem precedente[92].

Duas frases que se provaram verdade foram: "vamos tomar o poder, que é diferente de ganhar a eleição”[93] e “o Poder Judiciário não vale nada, o que vale são as relações entre as pessoas” – do ex-presidente réu criminal (des)condenado que restou impune, sem passar um dia sequer em cadeia real[94].

Bolsonaro prometia privatizar e reduzir gastos públicos e tributos, flertando com imposto único, fechamento do STF, cortes de “bolsas-vagabundagem” e armamento de fuzil para fazendeiros. O resultado após a maior parte do mandato foi:

1) ampliou o desarmamento, reduzindo o número e a natureza das armas que um cidadão comum pode ter no SINARM (sistema de registro de armas de cidadãos comuns), indicando para o MJ - Ministério da Justiça sucessivos agentes admiradores e ativistas da extrema-esquerda, que, por sua vez, aparelharam o MJ com desarmamentistas convictos[95];

2) no Ministério da Fazenda, como na maioria dos ministérios, indicou majoritariamente esquerdistas e gente comprometida com a extrema-esquerda – como a nomeação da família de Leo Pinheiro (um dos principais operadores do mensalão) para a CAIXA; de Gustavo Franco (íntimo de FHC e #elenão ativo na época da eleição) e Levy (ligado e indicado por Dilma e que estava no jantar de Cabral em Paris) para o BNDES; e de gente

do BTG (cujo controlador é ex-presidiário por ser "o banqueiro de Lula") para a maioria dos bancos públicos;

3) nas mudanças legais, ampliou os privilégios feministas[96], a engenharia social e a carga tributária, reduzindo a poupança e a renda privada com uma reforma da previdência imoral e estatista que pereniza a miséria;

4) o ENEM de 2019 foi amplamente considerado o mais vergonhoso, em sua desorganização, e progressista, em seu conteúdo, desde sempre[97] - e o de 2020, nem se fala;

5) em vez de combater o comunismo e cortar relações diplomáticas com ditaduras criminosas, Jair prometeu, em discurso na ONU[98], facilidades como o ingresso no país sem visto de agentes do regime mais assassino e genocida da história, enquanto seu vice propunha abertamente casamento do país com o Partido Comunista Chinês (PCC); e,

6) em vez de eliminar estímulos perversos[99] de "bolsas-farelo petralhas", que subsidiam o ócio e a informalidade, sancionou o maior programa de subsídio à vagabundagem com "Auxílio Emergencial" a mais de 66 milhões de pessoas[100] (excluindo qualquer empregado ou servidor) e, em ano eleitoral, propôs "imposto de renda negativo" para perpetuar esses pagamentos.

Resistir é desinvestir! Ter qualquer coisa em ditadura de exceção bolivariana é financiar e apoiar seus crimes. Quando o voto na urna é opinião da maioria são irrelevantes, relevantes passam a ser os "votos com os pés" (onde coloca o dinheiro) ou com armas (lutando para reconquistar as liberdades).

Os Estados Sociais hoje são deficitários (como previsto por Hayek) e não são sustentáveis. Eles tendem a se transformar em:

1) ditaduras totalitárias – como a China[101], com seu Estado policial com monitoramento e controle draconiano e milhões de vítimas em campos de concentração para retirada de órgãos[102] por crimes políticos, como ser cristão ou islâmico; ou 2) paraísos regulatórios e fiscais de portas abertas ao Bitcoin, seja vendendo cidadania sem imposto de renda (*St. Kitts*), residência com isenção perpétua (Zug) ou outros benefícios, como Gibraltar, Curaçao, Malta, Estônia, Paraguai, Portugal, Coreia do Sul, Japão ou El Salvador.

Desde a Antiguidade Clássica até os pais fundadores, reconhecia-se que a democracia é uma degeneração da República – tanto que nem empregaram o termo em sua Constituição, única a durar mais de dois séculos, com exceção da de San Marino. Tanto é uma corrupção da ideia da sociedade pública no “condomínio em que os porteiros votam” que a Coreia do Norte e a Alemanha Oriental, apesar de suas experiências criminosas, tinham “democrático” em suas denominações oficiais.

Hoppe demonstra que “a democracia virtualmente garante que somente os maus e perigosos cheguem ao topo do governo”, o que é comprovado nos casos de redução do Estado com explosão de riqueza e desenvolvimento em Hong Kong, Coreia do Sul e Cingapura. Isso não ocorreu onde havia democracia – mas, sim, legalidade e garantia de direitos à propriedade.

Também é demonstrado há décadas – tanto pelas escolas de economia política do *Public Choice* (Teoria das Escolhas Públicas) e de *Bloomington* – que é categoricamente impossível regenerar Estado de Exceção totalitário por vias institucionais e tampouco sem eliminar as “elites dirigentes” ou “grupos concentrados de interesse", como demonstrado no “Problema de Olson” (ou problema da ação coletiva). Para eles, as únicas alternativas a ditaduras de exceção são: votar com os pés (desinvestir e migrar); votar com armas (matar e arriscar-se a morrer); ou enfrentar a submissão, o terror e a miséria. Como todo confronto em que não há chance de acordo, as opções são fuga, luta ou submissão.

[Bitcoin é] muito atraente para o ponto de vista libertário se pudermos explicá-lo corretamente. Eu sou melhor com código do que com palavras.
Satoshi Nakamoto

É mais fácil o macaco mudar de árvore ou mudar a árvore de lugar?

Salvar a si mesmo é muito mais fácil que terceirizar a responsabilidade (terceirização moral) de salvar a sua família ou garantir seu sustento na velhice esperando um salvador da pátria ou melhorias institucionais que não ocorrerão. É assumir sua responsabilidade e fazer seu *hedge* ou *shortar* abertamente o que aponta para queda iminente. Aí,

restam o lucro e a tranquilidade, mesmo ao ouvir os absurdos da mídia oficial ou dos políticos eleitos.

A utilidade da informação não é perdida quando partilhada, por isso, PI (Propriedade Intelectual) é roubo[103] (sua natureza é violenta, vez que a única maneira de impor esses direitos é involuntária, por monopólio não contratual). Sinta-se à vontade para reproduzir parcial ou totalmente a obra, contanto que referencie a fonte.

Em uma lista de personalidades relevantes na comunidade, para busca de mais conteúdo, não podem faltar: Fernando Ulrich e Safiri Felix[104], grandes *speakers* de Bitcoin que produziram conteúdos muito didáticos para iniciantes. Richard Rytenband também tem excelentes materiais, como a série “Os Antifrágeis”, explicando a obra de Nassim Taleb capítulo por capítulo.

Há canais de resumos de notícias[105], como: “Visão Libertária”; Ideias Radicais (ressalvado que já elogiou a Atlas, pirâmide descarada e apaga vídeos quando muda de opinião[106]); Investidor Libertário (Roberto Pantoja); e KoreacomK[107] . Quanto a AT[108] (análise técnica), os principais atores em português são Guilherme Rennó e Fausto Botelho, acertam mais que erram, mas ambos já foram “oprimidos". Os “Bitcoinheiros”[109] são maximalistas de alto valor e reputação. Número de seguidores e *views* não são medidas de qualidade na Internet[110]: diversos golpistas e piramideiros têm centenas de milhares de seguidores - inclusive o *YouTube*, há anos, lucra com crimes e golpes anunciados na plataforma.

Há entes mais antigos na comunidade e com muito mais conhecimento técnico, reputação e horas dedicadas ao ecossistema que os autores, como Felipe Mica, Rodrigo Souza, Marco Carnut, Algorista, Daniel Fraga e Narcélio Filho. Se tiver dúvida sobre a reputação de alguém, verifique, pergunte a alguém em quem confie, construa sua rede de confiança[111] *(WoT - web of trust)*. Uma das máximas da comunidade é *“don’t trust, verify”* – não confie, verifique. “*Everyone is a scammer, and willpower is your only defense.*”

Rede de confiança (*WoT – web of trust*)[112]

Outras fontes em português recomendadas para quem passou do básico são: o “Café com Satoshi” (relatório quinzenal da Paradigma Capital); o relatório da NOX (além dos cursos de derivativos de João Paulo da Nox Bitcoin); 21 Milhões Podcast (João Grilo); *Foxbit Research* (relatório da Foxbit); Explica Bitcoin (@BitcoinExplica: traduções de artigos gringos sobre Bitcoin) e o portal *Livecoins*.

Em inglês, os principais canais do *Youtube* são: Keiser *Report*, C*ointelegraph*, *Cryptotips, BTC Sessions e Bitcoin Fixes This*, do Jimmy

Song.

Para um nível mais avançado, além das comunidades nas redes sociais, os *podcasts* de Stephan Livera, Laura Shin *(Bitcoin Unchained)* e o PeterMcCormack *(What Bitcoin Did Podcast)*, Anthony Pompliano *(The Pomp Podcast)*, Guy Swann *(Bitcoin Audible)*, Saifedean Ammous *(The Bitcoin Standard Podcast)* que têm crescido mais que os canais de *YouTube* e *Bitchute*. Uma etapa importante na educação em criptomoedas é cursar *MOOCs*[113] (cursos virtuais normalmente gratuitos), como da Universidade de Nicosia, ou o curso sobre Economia Austríaca e Bitcoin, da *The Bitcoin Standard Academy*, de Saifedean.

INTRODUÇÃO
A doença ponerológica e a cura criptográfica

"O futuro não chega para todos ao mesmo tempo." Ainda há pessoas que vivem em casas sem energia elétrica ou água encanada, se locomovem por tração animal e cozinham com lenha.

A criptografia[114] foi considerada arma de guerra por gerações. Entretanto, armas nas mãos de combatentes que não sabem quem é o inimigo, nem em que guerra estão lutando não têm valor algum. Essa introdução detalha algumas das ameaças que justificam o uso da criptografia como bote salva-vidas.

Demonstrações comuns disso são as pessoas que descobriram o Bitcoin cedo, tendo domínio de conceitos de TI, Teoria dos Jogos e até programação, mas que não entenderam suas implicações políticas, econômicas e sociais, perdendo a oportunidade de investir cedo tudo o quanto poderiam e deveriam.

O mundo está passando por uma mudança de paradigmas na produção, circulação e distribuição de riquezas, que alguns definem como Era Digital, Singularidade ou Economia da Abundância[115]. Essa revolução tecnológica, como as anteriores, vai reduzir brutalmente as margens das atividades superadas e promover uma transferência de riquezas sem precedentes.

Atividades que há poucos anos eram de alta tecnologia e retorno hoje sofrem processo de *commoditização* – até na fabricação de *hardware*, telecomunicações e desenvolvimento de *software*. Como resume Michael Saylor: em todas as épocas os melhores negócios são de alta tecnologia, margem está nos mercados ainda não competitivos.[116]

Neste ambiente, as formas convencionais de criar e acumular riqueza não funcionam mais. No passado, bastava gastar menos do que se ganhava e, sistematicamente, investir o excedente em fontes de renda – deixando o juro composto fazer o resto do trabalho.

Hoje não existem mais fontes de renda perpétuas, não existem mais investimentos seguros que garantam fluxos de caixa com retornos positivos sistemáticos e, provavelmente, todos os produtos financeiros convencionais têm expectativas de perda real. Essa disfunção alimenta a ética hedonística do consumismo e a irresponsabilidade, que induz as populações à miséria e ao voto nos estatistas, uma vez que, "quando se quer o impossível, apenas mentirosos podem satisfazê-lo".

Ora, foi pela falta de acesso a produtos financeiros idôneos a produzir ganhos que, por gerações, os investimentos prioritários do brasileiro (em especial de baixa renda) eram imóveis – para agropecuária no interior e para construção nas áreas urbanas (chegando-se ao ponto de haver mais lojas de materiais de construção que padarias).

Diante da queda da fecundidade e da massificação do comércio digital, as demandas por imóveis residenciais e comerciais tiveram suas tendências comprometidas. A agricultura profissional de pequeno porte se inviabilizou, como consequência da quebra da segurança jurídica no campo (vide ações terroristas impunes do MST – Movimento dos Sem Terra – e desarmamento covarde dos inocentes), da indústria de multas ambientais e da [in]justiça do trabalho.

O que aconteceu com quem vivia de alugar "placas de táxi"? O que aconteceu com a renda de quem alugava linhas telefônicas? O mesmo deve acontecer, cada vez mais rápido, em dezenas de setores – até o final da próxima década (considerando as curvas exponenciais), com os governos, suas moedas fiduciárias e todos os investimentos sob seu controle soberano.

Novas indústrias surgem com tecnologias da *Internet of Business (big data, blockchain, IOT, AR, VR, AI, analytics e cybersecurity)* a ponto de mais de 90% dos ganhos dos índices convencionais de ações dos EUA nos últimos anos serem de empresas ".com"[117] – com ênfase nas *FAANGs* –

com praticamente todos os demais setores tendo suas rentabilidades mitigadas. Isso denota a morte de grandes corporações e declínio de setores inteiros que eram dominantes há menos de uma década.

As ações tendem a ser substituídas por *equity tokens*, as moedas fiduciárias de governos por *cryptocurrency*, e sistemas democráticos por democracias societárias e sistemas de consenso ou holocráticos. A riqueza também tende a migrar dos ativos físicos para aqueles imateriais (como conhecimento).

O fim do sistema convencional – *legacy system* – não é evidente apenas na perda de lucratividade e eficiência das empresas tradicionais, mas também no esgotamento dos modelos governamentais, políticos e sociais em face do fim dos poderes estatais que os financiam.

As sociedades ocidentais vivem em crises morais, financeiras e demográficas – evidentes pelos níveis de fecundidade abaixo dos níveis mínimos de manutenção, pelos juros reais negativos, pela "Guerra ao Dinheiro” (com a progressiva ameaça de fim do dinheiro físico e totalitarismo financeiro) e pelo *déficit* sistemático e exponencial dos Estados Sociais (*welfare states*), demonstrando sua insustentabilidade e a iminência de seu colapso.

A pirâmide de Maslow[118] demonstra que, satisfeitas as demandas mais primitivas, novas demandas surgem hierarquicamente para os seres humanos. Quem está sendo sufocado por minutos não vai se preocupar em estar com sede por horas, e quem não tem água por dias não vai se preocupar com a fome.

Na verdade, ganhar dinheiro, ter sexo ou obter aceitação social só é uma grande preocupação nas camadas[119] iniciais da personalidade, ou seja, para aqueles que têm dificuldade de atingir esses objetivos. Quem ler e compreender os objetivos deste livro e ainda não for independente, vai avançar uma camada nesta pirâmide: vai vencer uma preocupação comum para liberar tempo e energia para questões superiores.

Hierarquia das necessidades de Maslow

Compreendendo esse conceito e observando como as prioridades médias da população têm descido para baixo na pirâmide referida, fica claro como a camada da personalidade média da população, o QI e o desempenho em testes de conhecimento informativo[120] têm decaído sistematicamente por décadas no Brasil.

Nenhuma sociedade com QI médio inferior a 90 chegou ao primeiro mundo e – com exceção de lugares que experimentaram o terror comunista – nenhum país com QI médio acima de 100 deixou de se tornar desenvolvido.[121]

As correlações entre baixa preferência temporal[122] (autocontrole de sacrificar benefícios no presente para usufruir no futuro), o alto QI e maior renda são observáveis em indivíduos e em populações, embora haja grande controvérsia entre a causalidade recíproca ou comum[123].

A destruição da inteligência não é o principal problema do país, ela é apenas uma consequência do processo ponerológico que implantou a patocracia[124] e o Estado de Exceção no país. A ponerologia é uma doença mental coletiva promovida pela engenharia social que utiliza o marxismo cultural como ferramenta de infiltração e subversão.

Para quem nunca teve contato com estes conceitos, as estratégias de inteligência dos grupos totalitários podem parecer "teoria da conspiração", mas essa é a explicação simples porque, nas mais diversas áreas do conhecimento e das políticas públicas, teorias e mitos refutados são tidos como verdades científicas e senso comum.

O fato é que as instituições brasileiras são aparelhos marxistas – como tribunais, mídia, academia e até igrejas – porque foram infiltradas e subvertidas por ações de contrainteligência por mais de 90 anos através de concursos fraudados ou enviesados e de assassinatos de reputação ou reais. Primeiro, pelo esforço soviético[125] e, após isso, por seus sucessores como o Foro de São Paulo[126]. Desta maneira, o cultivo da mentira, da falta de inteligência, da corrupção e da miséria foi planejado e executado como ferramenta de engenharia social.

Governos precisam de populações majoritariamente pobres, dependentes e submissas para manter seu poder. Se as pessoas forem independentes, ricas e céticas, elas vão atribuir poderes aos governos? Esta é a razão real de o governo controlar a educação e a moeda.

Evidência de como existe uma brutal diferença entre a verdade e as informações direcionadas para as massas é o indicador de preço que

funcionou com 95% de precisão (se interpretado no sentido inverso): foi a subida do preço do bitcoin quando a CNBC fazia reportagens negativas e a queda quando fazia manchetes positivas[127].

Uma demonstração objetiva de que o crescimento do Estado é uma ferramenta de engenharia social e não ocorre de boa-fé, pelo menos quando há psicopatas no poder, é a violação dos limites das curvas de Laffer e de Rahn[128] pela instituição de alíquotas mais altas que o ponto ótimo de arrecadação.

Como comprovado por extensa literatura, mesmo nos Estados Unidos, os governos poderiam arrecadar mais reduzindo os níveis de tributação e gasto público – mas não o fazem para satisfazer grupos lobistas, devido à captura administrativa.

Outra tendência da engenharia social, ressaltada por autores como Stefan Molyneux[129], como sinal do colapso civilizacional, é o relativismo moral, com ápice nas histerias transexualista, negrista, gayzista, pedófila, zoófila[130] e feminista[131] como pautas relevantes de debate político e com super estímulo à promiscuidade e castração em crianças.

Um dos fatores cruciais que inviabilizou a manutenção da escravidão em sociedades cristãs, embora esse fosse um instituto mencionado e reconhecido na Bíblia, foi a restrição moral à promiscuidade. Escravos que têm relações monogâmicas passam a ter relações conhecidas de parentesco e, formando famílias, passam a ter pessoas dispostas a matar e a morrer umas pelas outras e a ter identidade ancestral.

Por isso, sociedades com quantidades significativas de escravos só conseguiam mantê-los escravos através de esquemas obrigatórios de cobertura por múltiplos parceiros – eliminando as relações monogâmicas e, consequentemente, destruindo o núcleo de proteção e estrutura social básica – como em Roma e na Grécia Clássicas[132].

Autores como Rollo Tomassi[133], Stefan Molyneux[134] e Olavo de Carvalho também ressaltam que um dos fatores-chave para a queda da fecundidade – que sentenciou as previdências de repartição ao colapso – foi a liberação sexual e a instituição de leis subvertidas feministas[135], obliterando as motivações de homens e mulheres para manterem famílias estruturadas[136].

Mesmo bilionários como Saylor simplesmente desistem de casar, estilos de vida como *herbs* japoneses *e MGTOW* são, cada vez mais comuns. A sua argumentação[137] é simples: as leis inviabilizam contratos viáveis de casamento, de modo que governos feministas garantem estímulos ao maximizar o oportunismo hipergâmico. Em outras palavras, o governo é uma máquina de transferir riqueza e poder de produtores (a maioria homens) para dar a beneficiários de renda estatal (a maioria mulheres), como é óbvio pelos dados de pagamento de impostos ou até mesmo contribuições e benefícios previdenciários[138].

Historicamente, o que um homem poderia oferecer como homem era segurança – física, material e emocional – e o que uma mulher poderia oferecer era fertilidade - aferida por atributos físicos - e fidelidade. Por isso virgindade é ativo para mulher e passivo para o homem no cálculo do valor sexual e, de maneira inversa, a promiscuidade[139].

Essa troca ficou inviabilizada com leis feministas atuais, como a absurda e antinatural paternidade involuntária por *DNA*, fomentando o golpe da barriga, promiscuidade[140] e nascimentos fora do casamento - a ponto de Molyneux denominar o *welfare state* como *single mom state*[141], devido a

altíssima correlação entre desestruturação familiar (e moral) e o aumento do Estado Social.

As mulheres não precisam mais de segurança do homem (agora, provida oficialmente pelo Estado, em cada um dos aspectos). Os homens, sem qualquer garantia de fidelidade e com amplo acesso a sexo com custo marginal quase zero, não têm motivação para investir em procriação de filhos[142] sob os quais não terão poder, comprometendo sua renda por décadas e que podem até não ser deles[143].

Segurança física é o que explica as filas de mulheres jovens e bonitas para "visitas íntimas" nas cadeias. Uma vez que sejam mulheres de bandido filiado à facção passam a ser protegidas até mesmo de “talaricagem” no tribunal do crime. Fora do ambiente controlado por facção criminosa assumida, o protetor da mulher é o Estado que faz propaganda afirmando que seu marido ou seu pai é agressor e estuprador em potencial e deve ser denunciado ao Estado.

Segurança material é o homem exercer papel de provedor. Com mulheres ganhando mais e tendo mais instrução que homens, graças à explosão de assistencialismo, distorções e gastos públicos do Estado “gigolô”, as mulheres não precisam mais de provedor.

Dalvana, que isso... na nossa casa...

Deixe de ser machista, Carlos, são novos tempos.
Eu não tolero isso, acabou. Vá embora, a casa é minha.

Alô, polícia? meu marido machista está me agredindo psicologicamente, socorro!

Não resista, cidadão, vai virar putinha na cadeia, machão!
E aí, pessoal do insta, tamos aqui agora prendendo esse machão agressor de mulher, arrasta pra cima!

Ainda pior, com mais instrução e renda, a mulher tende a se avaliar muitos pontos acima do seu real valor sexual de mercado[144], ficando alienada (na busca por relacionamentos, mesmo conseguindo muitos parceiros sexuais), por nunca encontrar um par que ela julga digno para compromisso (e que a aceitaria). Ainda pior quando é enganada pela promessa de estabilidade de “previdência”, “cargo público" ou "herança".

Essa é a gênese usual das “tias dos gatos” e das “mães de *pets*”[145].

Humanos também são animais, seus comportamentos têm aspectos evolutivos etnobiológicos[146] consolidados em milhares de anos de pressões seletivas: homens serem homens, mulheres serem mulheres e humanos serem seres gregários e tribalistas. Quando normas jurídicas inviabilizam o exercício dos comportamentos naturais — contrariando o direito natural e o PNA[147] — as famílias, comunidades e países se degeneram — com destruição das instituições, queda da fecundidade, diluição da moeda e da moral[148]:

Por isso, os governos e corporações estimulam a degeneração dos valores morais e éticos, por meio de leis de alimentos e pensões, bolsas assistencialistas (que não permitem ascensão dos mais pobres, mantendo-os eternamente na pobreza), privilégios a grupos de poder (incluindo minorias intolerantes) e campanhas “culturais” subversivas[149]. A finalidade é única e simples: obter mais e mais votos e ativistas para partidos de extrema-

esquerda, alimentando o ciclo de mais impostos para os produtores e mais auxílio aos parasitas.

Outro exemplo da histeria e infantilização coletiva usadas em prol de interesses corporativos e estatais é a preocupação com falsas questões ambientais, como na década de 1980, com o “buraco na camada de ozônio”, ou a mania atual do “aquecimento global”, rebatizado para “mudanças climáticas” – desmoralizada recentemente pela descoberta de processos como o “escurecimento global”[150].

Ora, sobram evidências de que a Terra já foi muito mais quente e mais fria, muitas outras vezes; e, havendo ou não havendo “mudanças climáticas”, a sociedade vai se adaptar muito melhor sem regulações estatais do que com elas[151].

Ademais, os maiores desastres ambientais da História provocados pela humanidade foram causados por Estados totalitários[152] e não por empresas – vide Chernobyl, Kyshtym[153] e o Mar de Aral na URSS, e a grande ideia de Mao Tsé-Tung de matar pardais (Campanha Mate um Pardal), provocando a grande fome na China[154] – a ditadura comunista é campeã atual em qualquer tipo de passivo ambiental[155].

O Efeito Gell-Mann de Amnésia[156] ilustra como pessoas altamente instruídas aceitam fontes refutadas por elas mesmas, desde que em temas nos quais não sejam especializadas.

Desde Hayek (para não dizer desde os *founding fathers*), qualquer jurista de respeito entende que só existem direitos públicos negativos[157] e promessas de saúde e educação públicas são o “caminho da servidão”, levando inevitavelmente ao totalitarismo. Qualquer médico ou nutricionista com formação mínima sabe que os mitos – acerca das gorduras saturadas, sal e fibras – difundidos por Ancel Keys são mentiras descaradas[158]; como afirmações de que pecuária é prejudicial ao meio ambiente[159], qualquer economista decente entende que o “ambiente intelectual” de keynesianismo e marxismo só leva a mais estatismo, subdesenvolvimento e pobreza. Agora, cada um deles, embora entenda que o “senso comum” ou “discurso convencional” sobre sua área seja um monte de mentiras refutadas, ainda tende a dar crédito pleno às mesmas fontes (academia, mídia, governo...) nos demais temas.

O grupo de *Cypherpunks* no qual o Bitcoin começou já compreendia o entendimento de Hoppe de que a *Democracia é o deus que falhou*. Na

verdade, há muitos exemplos de democracias funcionais – como as societárias –, embora até mesmo os *founding fathers*[160] tivessem ojeriza a este termo, evitando-o na Constituição Americana e utilizando o termo "República". Assim como a adoração pelo termo "democracia" por ditaduras totalitárias e assassinas como a "República Popular **Democrática** da Coreia" (Coreia do Norte) e a "República **Democrática** Alemã" (Alemanha Oriental).

Uma democracia em que os beneficiários líquidos (parasitas em linguagem ecológica) votam e têm maioria é como um condomínio em que os porteiros e visitantes votam.

Ora, os porteiros e visitantes, que não pagam condomínio, vão sempre votar para que sejam ampliados seus benefícios e as taxas condominiais – até que as unidades percam todo o seu valor e o condomínio quebre. Esse é o resumo do que é um Estado Social e por que todas as experiências de dar saúde e educação "gratuitas" sempre terminaram em tragédia, terror e miséria desde a República de Weimar até a atual colonização da Europa pelo Islã – através dos *welfare magnets*, que impõem a *sharia* e sua cultura de violência e estupro sistemático de mulheres ou crianças "infiéis".

Nassim Taleb[161], em sua obra magna *Skin in the game*, demonstra os riscos inerentes à dissociação do controle e propriedade — e da tomada de decisões sem a assunção de consequências.

Essa dissociação já era demonstrada, há gerações, como a causa primária da corrupção na Teoria da Agência e na compreensão dos axiomas de Klein e Jensen-Meckling (contrato e dos agentes imperfeitos), mas eles ainda não permearam o "ambiente intelectual" o suficiente para que haja o entendimento corrente de que a única maneira de reduzir a corrupção e promover o desenvolvimento é reduzir o Estado e seus poderes.

As pessoas respondem a motivações, como demonstrado por Douglass North[162] e outras fontes da Economia Institucional: o que faz um país ser desenvolvido ou subdesenvolvido são suas instituições; sistemas em que comportamentos dominantes são oportunistas levam à corrupção endêmica e ao subdesenvolvimento. Por outro lado, onde há governança privilegiando a cooperação como comportamento dominante, tem-se desenvolvimento.

O Bitcoin possibilita que pessoas que vivem em qualquer país, por mais corrompido e subdesenvolvido que seja, possam usar uma reserva de valor e meio de pagamento capaz de mudar suas motivações em relação a

preferências temporais. Isso pode levar o mundo a uma nova era de produtividade e progresso – material, ético e tecnológico.

Ammous[163] também explica detalhadamente que a decadência das artes, inteligência, moral, famílias, impérios e até da saúde mental das populações é altamente correlacionada com a ausência de *sound money* – dinheiro sonante, capaz de ser reserva de valor – e de baixas preferências temporais decorrentes dele.

Então, se o leitor quer investir em alta cultura e considera que a guerra cultural é a primeira a ser vencida, entenda que o primeiro passo para isso é a adoção de uma boa reserva de valor que mude as motivações e, consequentemente, reduza as preferências temporais. E, o segundo passo, é o desinvestimento dos ativos que o leitor tem no domínio do inimigo, o *legacy*.

Para um país, uma empresa, uma família ou um indivíduo, os elementos fundamentais para a determinação de crescimento são acumulação e produtividade. Por motivos óbvios, no Brasil, os níveis de produtividade em relação ao resto do mundo e os níveis de poupança apresentaram quedas sistemáticas nas últimas décadas – e com o envelhecimento da população e a deterioração das instituições, a tendência é piorar.

A produtividade é determinada por diversos fatores – inclusive tem significativa correlação com poupança; mas um determinante simples dela em populações é o QI[164]. Poupança também é submetida a diversos fatores, mas o que pode servir de preditor imediato são as preferências temporais[165] baixas.

Só para dar um exemplo de como o Brasil é um país improdutivo: segundo dados oficiais[166], menos de 25% das terras são produtivas (somando cidades, agricultura, infraestruturas e pecuária) – enquanto a maioria dos países desenvolvidos empregam mais de 75%. Para piorar, no caso de “Banânia”, mesmo nesta fração útil, a produtividade ainda é baixíssima, com pouco uso de mão de obra (inviabilizada pela legislação trabalhista engessada) e tecnologias de ponta (inviabilizada pela regulação e tributação sufocantes).

Os níveis de eficiência e produtividade da utilização da mão de obra não são melhores (dados os níveis absurdos de inatividade, como os *nem-nem*[167] – nem trabalha e nem estuda –, eternos estudantes e desempregados) e tendem a piorar com o envelhecimento.

É uma demonstração de ignorância ou má-fé pessoas advogarem por determinação da taxa de juro pelo governo ou pela redução da taxa SELIC para estimular a economia. Ora, o brasileiro que viveu os congelamentos de Sarney e que testemunhou as experiências semelhantes de Maduro na Venezuela sabe muito bem quais as consequências do controle de preços – escassez e miséria. Governo determinar taxa de juro é imoral e economicamente pior que tabelar o preço do pão ou do feijão, pois se pode viver sem pão ou feijão (existem substitutos), mas não se pode viver em uma sociedade com curso forçado sem tocar em moeda estatal.

Se o governo pretendesse realmente reduzir as taxas de juro para fomentar a atividade econômica de maneira sustentável, ele iria cumprir suas funções próprias (jurisdição e defesa), aumentando e facilitando os meios de defender a propriedade privada e de executar devedores.

Desta forma, é importante frisar que consumo não produz crescimento sustentável, investimento sim. Maior consumo significa menor investimento – ou seja, menor produtividade futura.

Acumulação e propriedade não devem ter "função social" além de satisfazer as preferências do dono. Até mesmo Jesus, na Parábola dos Trabalhadores das Vinhas[168], deixa claro como é má e pecaminosa a pretensão de regular contratos voluntários alheios como faz a legislação trabalhista.

Quando alguém utilizar expressões como "função social", "empoderamento", "politicamente correto", "todes", "tod@s" ou "apropriação cultural", já se pode identificar uso da novilíngua marxista para conquistar corações, mentes e, é claro, poder – aquele texto estará reproduzindo linguagem ponerológica de maneira instrumental para desinformação.

Desta maneira, os idealizadores do Bitcoin compreenderam que, o início dos processos de *QE*, "alívios quantitativos", representava o passo final de captura administrativa das corporações sobre os governos, e, em consequência, a última chance das populações de evitar o totalitarismo financeiro com o fim do dinheiro físico e das chances de enriquecimento pela acumulação honesta.

Como demonstrava Bastiat no século XIX, ou Ron Paul no século XX, todas as funções dos Bancos Centrais são mais bem desempenhadas por instituições privadas (ou por ninguém). A emissão de dinheiro é uma

questão importante demais para ser deixada na mão de políticos, assim como a educação[169].

Rothbard[170] ilustra outro aspecto da subversão dos valores morais com o “educacionismo”, o mito de que as pessoas devem crescer na vida através da instrução formal, controlada e financiada por governos que aparelham as “escolas” com agentes de doutrinação e manipulação – os *intelectuals yet idiots*, de Taleb.

O aumento exponencial do Estado – usando como justificativa mais regulações para resolver falhas regulatórias anteriores (Lei de Michels[171]) até criminalizar todos na sociedade – dá ao governo o poder de punir quem quiser a qualquer momento legalmente[172]. São políticas com fito de provocar emigração de dissidentes (efeito Curley[173]) e a "Estratégia Cloward Piven” (aumentar obrigações financeiras do governo para provocar o colapso do país e a inevitável adoção de totalitarismo).

Se o Bitcoin sobreviver por mais uma década, ele será um bote salva-vidas para todos esses processos. É o mecanismo de proteção (*hedge*) fundamental contra os processos de insanidade coletiva, corrupção, totalitarismo e endividamento endêmicos; e, por isso, é elemento fundamental em qualquer carteira – não apenas por ser imperativo moral, mas para evitar risco de cauda (risco de ruína perdendo tudo quando o sistema convencional colapsar).

Por isso, até Taleb reconheceu que “o Bitcoin é o início de algo grandioso: uma moeda sem um governo, algo necessário e imperativo”.

Como será a seguir demonstrado, o Bitcoin muda as motivações de seus usuários, alonga suas preferências temporais, faz explodir sua produtividade e capacidade de acumulação e, se continuar seu curso de adoção exponencial, pode salvar o mundo do coletivismo – instaurando um novo entendimento do dinheiro e da moeda, da ética do trabalho, acumulação e relação com governos, e de respeito aos direitos alheios, superando mitos, mentiras e instituições corrompidas que atrasam o desenvolvimento da humanidade.

O Bitcoin será morto ou será a *causa mortis* dos Estados Sociais[174] – com a vitória do indivíduo sobre as ditaduras e corporações corruptas. Para isso que foi concebido.

Não é possível manter sob escravidão pessoas armadas e determinadas a serem livres, como Massada demonstrou. Satoshi expressou isso ao afirmar que “em algumas décadas, o subsídio será muito pequeno e as tarifas de

mineração serão a principal remuneração pelos nós de mineração. Estou certo de que em 20 anos haverá um volume de transação muito grande ou nenhum volume”. É vencer ou morrer.

Quando a maior parte da riqueza não puder ser expropriada, controlada ou mesmo ter titularidade suspensa por governos ou tribunais, não haverá como recolher tributos involuntariamente. Penas ou multas, e a ação estatal involuntária não terão mais sentido, viabilidade ou efeito prático.

Com o aumento exponencial dos dados e poderes acumulados por governos e corporações, o mundo se encontra às vésperas de um meio-termo entre as distopias descritas em *1984* e *Admirável Mundo Novo*. Quem quiser evitar viver o drama da *Revolução dos Bichos* terá que se evadir da fazenda antes das fases finais da Revolução – e o Bitcoin é uma das tecnologias úteis para evitar o domínio totalitário e para facilitar a fuga de onde o totalitarismo não possa ser evitado.

É uma guerra de extermínio. A cultura vencedora deste *fork*[175] social será o modelo a ser perpetuado nas futuras gerações. Não tem acordo ou meio termo, não tem prisão nem rendição. Você será livre como nunca sonhou ou escravo como ninguém nunca foi.

CAPÍTULO I: *5W2H*

Septen circuntantiae: *Quis, quid, quando, ubi, cur, quem ad modum, quibus adminiculis*. (*Who, what, when, where, why, in what way, by what mean*s.)

Em qualquer investigação, há um conjunto inicial de questões a serem respondidas ao investigar qualquer fato, *5W2H*: *Who, What, Where, When, Why, How, How Much* – derivadas das sete questões aristotélicas difundidas por São Tomás de Aquino. Vamos às respostas objetivas:

1 (Who/Where/When) - Quem criou o Bitcoin, onde e quando:

O Bitcoin foi proposto em um artigo *(Bitcoin: a Peer to Peer Electronic Cash System*[176]) enviado por um participante[177] que utilizava o pseudônimo de Satoshi Nakamoto (2008) em um grupo de *e-mails* de *cypherpunks*. Em 18 de agosto de 2008, o domínio bitcoin.org foi registrado, em 31 de outubro, o *whitepaper* publicado e, em janeiro de 2009, o código aberto foi divulgado, momento em que o sistema começou a rodar, com a mensagem *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"* registrada no primeiro bloco em 3 de janeiro de 2009.

Nesse grupo, congregavam os principais *cypherpunks*, *experts* em criptografia e ativistas do austro-libertarianismo e, em decorrência disso, o espaço era utilizado por alguns de seus participantes como meio de divulgação e teste de *softwares* abertos e descentralizados, em grande parte como resposta aos abusos reincidentes por parte dos governos dos seus privilégios de senhoriagem e monopólio de emissão de moeda. Os integrantes desse grupo sabiam que o domínio da criptografia pelo indivíduo médio era um fator fundamental para evitar o totalitarismo, como fica claro no *Manifesto Cripto Anarquista*[178], de Timothy C. May.

Os austro-libertários, como diversos grupos liberais clássicos e conservadores, até o desenvolvimento do Bitcoin, sempre defenderam o *gold standard*, o princípio de limitação da emissão de moeda às reservas de ouro de cada país, que evita inflação e preserva o valor da moeda corrente.

Usualmente, as civilizações em colapso acompanharam políticas destruidoras de valor, como tabelamento de preços e *déficit* sistemático, que

só foram possíveis por meio da diluição do valor da moeda, desde o Édito Máximo de 301 A.D. (homólogo à tabela da SUNAB em Roma), com a diluição exponencial dos denários desde Diocleciano e Nero até as práticas semelhantes nos governos de Nixon, Sarney, Kirchner, Maduro e Chávez.

> O problema raiz da moeda convencional é toda a confiança necessária para fazê-la funcionar. O Banco Central deve ser confiável para não desvalorizar a moeda, mas o histórico das moedas fiduciárias está cheio de violações dessa confiança.
>
> Satoshi Nakamoto

Após propor o *whitepaper* e contribuir ativamente na comunidade nos primeiros anos, Satoshi Nakamoto se despediu e deixou o projeto que continuou de maneira descentralizada[179]. Os primeiros bitcoins minerados, supostamente por ele, não foram movidos – servindo de prova de segurança das carteiras mais modernas e de garantia de que o criador até hoje não obteve vantagem pecuniária pela venda dos primeiros *tokens* criados.

Em que lugar fica o Bitcoin? Todos os registros de transações se encontram em cada nó (*full node*)[180], que totalizam mais de 10 mil usuários com o cliente instalado (*nodes ou nós públicos*)[181]. Desta maneira, o Bitcoin não está em nenhum país ou jurisdição específica, mas, sim, nas nuvens[182]. Um ótimo artigo chamado “A fabulosa ilha Bitcoin”[183] (2015), escrito por Felipe Micaroni, explica muito bem o processo de forma didática e lúdica.

> Uma ordem monetária espontânea emerge das interações complexas; não é algo conferido por debate acadêmico, planejamento racional ou mandato do governo.
>
> Saifedean Ammous

2 (What) - O que é o Bitcoin

Em apenas uma frase: bitcoin (*token*) é o dinheiro que pode ser enviado por qualquer meio de comunicação[184] e Bitcoin é o sistema público e aberto de registros de seu *token* nativo e o *software* livre para sua utilização pela Internet.

Por isso se afirma que para proibir o uso de bitcoins, globalmente, seria necessário destruir a Internet em todos os países do mundo; ou, em uma jurisdição determinada, impedir o direito de expressão, retirando dessa população rádio, *SMS*, telefone, carta e qualquer outra forma de comunicação com pessoas quem tenham acesso à Internet.

Direito com "D" maiúsculo é o sistema jurídico, conjunto de normas; e direito com "d" minúsculo é a faculdade legal. De maneira análoga, Bitcoin com "B" maiúsculo é uma plataforma, constituída de um *software* aberto e livre, com milhares de atores validadores e processadores (nós e mineradores) em um sistema de registro descentralizado[185] denominado *blockchain* ou *timechain;*

Esse sistema já consome mais energia que vários países e possui o maior poder de processamento do planeta — cerca de 89 milhões de *terahashes* por segundo (TH/s) em maio de 2021, cerca de 100 vezes maior que os servidores do Google.

O Bitcoin como sistema é composto por: a) **nós (nodes)**, atores que mantêm os registros das transações passadas (memórias registrando e validando todas as transações); b) **mineradores**, processadores remunerados com os novos bitcoins (subsídio) e taxas voluntárias (*fees*) por disponibilizar poder computacional para processar transações e garantir segurança da rede; e **c) usuários** (entes que usam o sistema, enviando e recebendo saldos)[186]:

Money Over Internet Protocol

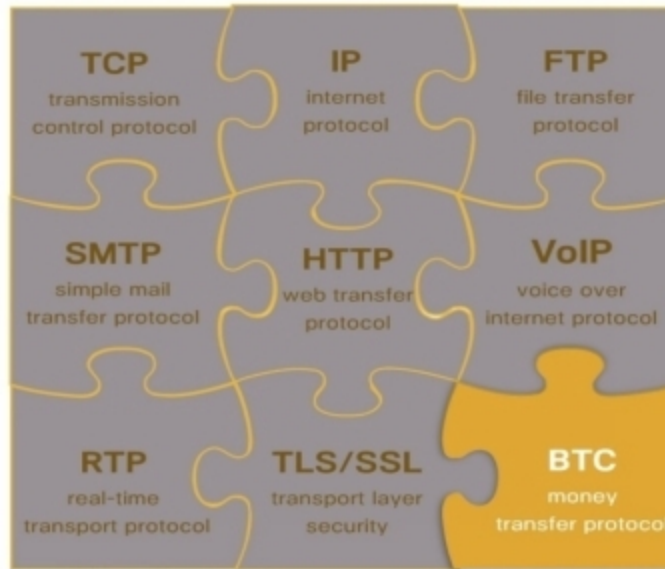



Image from Pantera Capital

O bitcoin com “b” minúsculo é a unidade básica do sistema (*token*), com a qual são pagas taxas (*fees*) para uso e com a qual os serviços de mineração são remunerados. O bitcoin é o “dinheiro digital”, “ouro 2.0”, “dinheiro mágico da Internet”, moeda sem terceiro de confiança (sem garantia de Estado, Banco Central, empresa, *CEO*, nem servidor central), baseada não em entes, mas na confiança em motivações no sistema descentralizado de governança e no *software* proposto por Satoshi Nakamoto[187], operacional há mais de 11 anos.

O Bitcoin tem três funções inatas: a) é sistema de comunicação global, incensurável, público e perpétuo – que garante a faculdade de troca de informações e registro público de dados fora de qualquer controle estatal; b) é sistema de pagamentos que não está sujeito às jurisdições nacionais, o que inviabiliza, na prática, controles de capitais (incluindo no mercado internacional os bilhões de indivíduos sem acesso a serviços bancários); e c) é plataforma de manutenção de saldos como reserva de valor, que apresenta certas características de dinheiro superiores ao ouro e a qualquer reserva de valor anteriormente adotada – libertando seus usuários de expropriações e tributos involuntários, mesmo após a sua morte, incluindo aí até mesmo a senhoriagem e a inflação.

Fernando Ulrich[188], em 2014 e 2015, publicou no *Infomoney* dois textos fundamentais para a popularização no Brasil: *Dez formas de explicar o que é Bitcoin*[189] e *Guerra ao dinheiro, juros negativos e a crise na Grécia*[190].

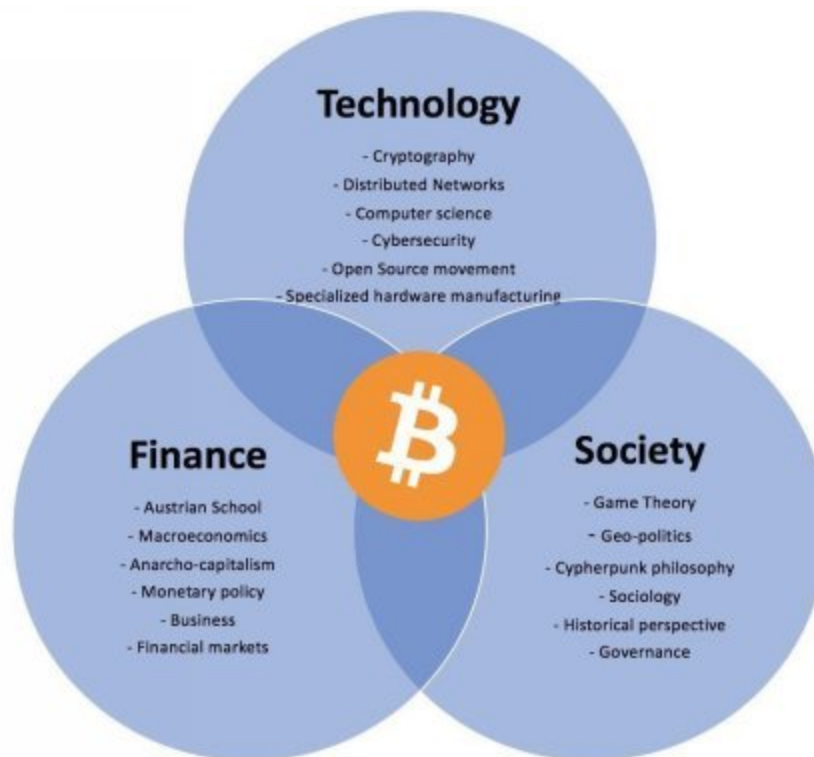
O Bitcoin não é uma democracia. Ele utiliza um padrão de governança superior de decisões por unanimidade em que não há sanções violentas, mas apenas motivações baseadas em Teoria dos Jogos e Teoria das Escolhas Racionais. Essas características o tornam sistema dominante para comportamentos cooperativos e inibem financeiramente o oportunismo[191].

Satoshi[192] demonstra que “a quantidade é uma qualidade em si mesma", quando define o bitcoin como uma mercadoria que tem potencial de valor derivado da raridade e da transportabilidade. Em livre tradução:

> Como um experimento mental, imagine que houvesse uma base metal tão escassa quanto o ouro, mas com as seguintes propriedades: cor cinza; não é um bom condutor de eletricidade; não é particularmente forte, nem dúctil ou facilmente maleável; não é útil para nenhuma finalidade prática ou ornamental, mas tem uma propriedade mágica especial: Pode ser transportada por um canal de comunicação. Se, de alguma forma, adquirisse algum valor por qualquer motivo, qualquer pessoa que desejasse transferir riqueza a uma longa distância poderia comprar um pouco, transmiti-lo e pedir ao destinatário que o vendesse.

Satoshi também deixa claro nos fóruns, no *whitepaper* – e não apenas no Bloco Gênese – que o Bitcoin foi criado para a eliminação dos problemas do terceiro em pagamentos digitais e da degradação da moeda convencional. Em livre tradução:

> Eu desenvolvi um novo sistema de *e-cash P2P* de código aberto chamado Bitcoin [..] – completamente descentralizado – nenhum servidor central – sem partes confiáveis – baseado em prova de criptografia em vez de confiança – problema com moeda convencional é [degradação]...

Como ilustrado[193], o Bitcoin é uma combinação de várias tecnologias e conceitos: Economia – Teoria Monetária – Teoria dos Jogos – Criptografia – Computação – Redes distribuídas e outras, como fica demonstrado no *whitepaper* escrito pelo idealizador, Satoshi Nakamoto:

Como demonstrado por Parker Lewis, a compreensão do Bitcoin é um processo lento, assim como a construção de uma infraestrutura, em um ciclo virtuoso ilustrado pelo esquema[194]:

Conhecimento → Infraestrutura → Adoção → Valor →
Conhecimento → Infraestrutura

Logo que o usuário iniciante, *noob*, entende o que é o Bitcoin, algumas questões acerca de sua natureza são típicas: bitcoin é pirâmide? Qual o lastro do bitcoin? Bitcoins vão substituir totalmente as *fiats* (moedas estatais)? O Bitcoin não foi hackeado ou fraudado? Será destruído pela computação quântica? Quando eu morrer, para onde irão meus bitcoins? Era vantagem comprar no início, não agora! Não é melhor comprar a *shitcoin* que custa apenas 1 satoshi em vez de bitcoin?

Pinned Tweet
Willy Woo @woonomic · Jun 13
Fiat: 48.8 years old
Bitcoin: 11.4 years old
In case you're wondering, fiat money is also an experiment.
145
875
3.7K
Show this thread

2.1 Bitcoin é pirâmide? Bitcoin é ilegal?

No Brasil, a propriedade e uso do bitcoin são legais e regulados por normas infralegais como a IN nº 1.888 da Receita Federal. Há países que criminalizam e reprimem sua mineração, como a ditadura totalitária da Venezuela[195].

Há dezenas de bandidos que usam o bitcoin, do mesmo modo que há incontáveis esquemas ilegais que usam reais, dólares, euros e toda espécie de ativo.

Não se pode confundir a moeda ser criminosa com a moeda ser usada por criminosos. De fato, o crime usualmente adota tecnologias mais rápido que outros setores. Há registros públicos e notórios de mais e mais atividades criminosas utilizando bitcoins. Inicialmente eram os estelionatários, agora também usam os sequestradores[196] e os “empresários” ligados ao MBL[197].

A lei brasileira não define o que é pirâmide, embora desde 1951 (Lei 1.521/51, art. 2, IX) puna até mesmo a participação em "pichardismo", "bola de neve" e "quaisquer outros equivalentes", como se existisse analogia em tipificação criminal.

Segundo a justificativa da lei, Manuel Severo Pichardo[198] fazia o mesmo esquema que Charles Ponzi fazia nos EUA: ambos ofereciam retornos acima do mercado sem ter qualquer produto, pagando os antigos investidores com a grana dos novos. No primeiro dia que saírem mais recursos que entrarem, os operadores do esquema sumirão (*exit scam*), quebrando com o lucro concentrado no topo e o prejuízo na base, por isso a metáfora da pirâmide.

Nessa definição, o INSS seria um grande exemplo de pirâmide (ainda mais imoral por ser obrigatório). Restaria inviável se não fosse a faculdade de o governo imprimir sua moeda soberana o quanto quiser, diluindo o valor das vítimas que a acumularam. Isso sem contar que a fecundidade e os índices de contribuintes previdenciários só fazem cair. O passivo aumenta e os ingressos diminuem sistematicamente, garantindo o calote branco.

O Bitcoin não é uma empresa, não tem um responsável, ninguém promete retorno algum e o ecossistema passa meses liberando mais grana do que entra no mercado sem deixar de operar e ter liquidez (na verdade, o bitcoin passou 2x mais tempo em baixa que em alta).

Além disso, o bitcoin é um ativo que tem valor derivado da sua utilidade e não de qualquer promessa, devido às suas propriedades intrínsecas (fungibilidade, durabilidade, divisibilidade, portabilidade e escassez). Por isso, não satisfaz nenhum dos três critérios de “pirâmide”.

É provável que sua aposentadoria, herança, cargo, renda ou concessão públicas não existam ou não tenham valor significativo em 25 ou 35 anos, devido a questões estruturais (disrupção tecnológica com evolução exponencial) e questões políticas (colapso dos Estados Sociais com proliferação de paraísos regulatórios e fiscais e ditaduras totalitárias sem precedentes). É melhor para quem é credor (presente ou eventual) do Estado (nem que seja de expectativa de direito) ter 5-10% do patrimônio em bitcoin ou arriscar a perda total apostando tudo na solvência futura e eventual de devedor que já é insolvente?

Talvez o Bitcoin não exista mais em 20 anos, mas, se ele existir, servirá de *hedge* devido às suas características idiossincráticas e à baixa correlação com ativos convencionais (que justificam a tese[199] de "nova classe de ativo").

2.2 Qual é o lastro do Bitcoin?

O *Gold Standard* deu errado todas as vezes em que foi tentado, até o choque de Nixon em 1971 e o fim do acordo de Bretton Woods[200]. Em todas as vezes que algum governo ou banco emitiu, por tempo ou volume significativos, moeda escritural ou *IOU* (I owe you) supostamente conversível em ouro, houve calote, formal ou branco. Esta é a razão de o Bitcoin ter sido criado: sistemas baseados em confiança falharam sistematicamente por milênios.

Lastro como garantia de escassez é o *software* que limita sua emissão e seu sistema de governança para que cada nó siga a regra que quiser. Se eventualmente usuários decidirem que a emissão de bitcoins vai aumentar (ou quiserem mudar qualquer outra regra), aqueles que não concordarem podem continuar rodando seus nós com as regras originais, gerando um *fork* (divisão da rede, como ocorreu mais de uma dezena de vezes como o *bitcoin cash* e o *bitcoin gold*). Até hoje, todos os *forks* deram prejuízos aos dissidentes e lucro aos *holders* que desovaram as "moedas grátis" nas primeiras horas em que eram listadas.

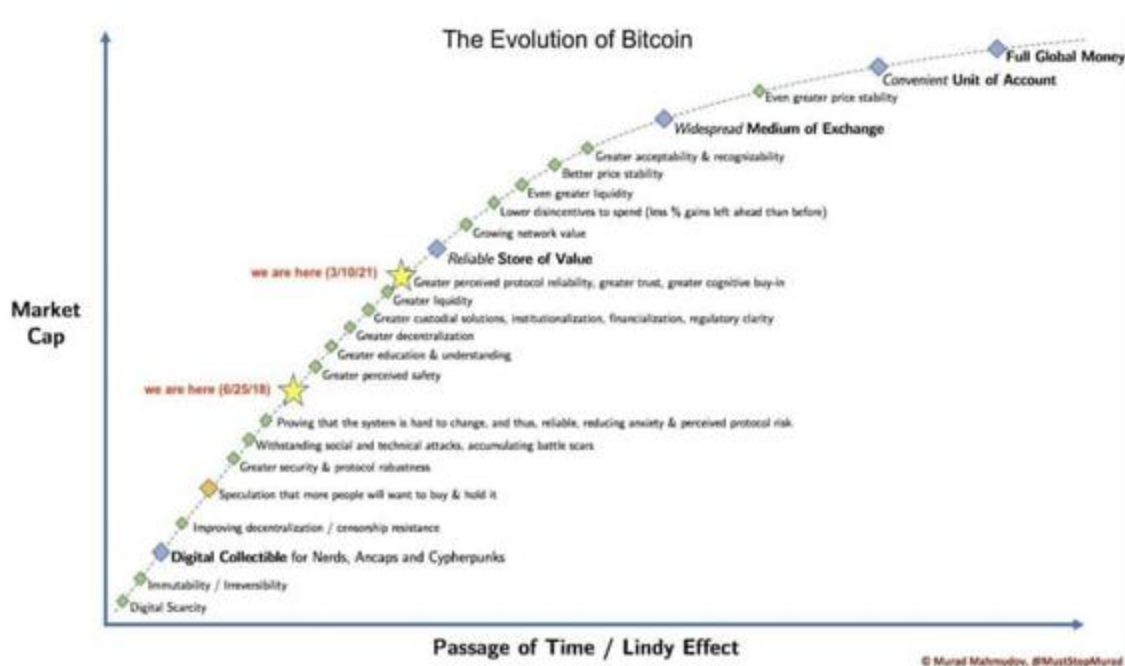
Lastro como valor-utilidade é derivado das suas funções (reserva de valor imune a expropriação, transações, controles de capitais e sistema de registro e comunicações incensuráveis) e é diretamente proporcional a abusos estatais em tabelamento de preços, censura, expurgos, diluição da moeda, controles de capitais e *déficits* em orçamentos públicos. Por isso, acredita-se que, se o *gold standard* fosse respeitado, o Bitcoin nunca existiria.

Lastro como conversibilidade é a possibilidade de usar o *token* para fazer transações e registros públicos (graças aos bilhões em investimento irrecuperáveis em *ASICs* dos mineradores, profissionais comprometidos, empresas do ecossistema e toda infraestrutura).

As moedas fiduciárias não têm lastro de conversibilidade (quando não estão em regime de paridade com outra *fiat* ou com emissão limitada por *currency board*) e não têm lastro como garantia de escassez, só tendo algum valor porque os tributos têm que ser pagos em *fiat* e devido ao curso

forçado (*legal tender*) – a obrigação legal de as vítimas aceitarem a moeda como pagamento ou sofrerem violência.

2.3 Bitcoin vai substituir as moedas estatais?

Como ilustrado na figura “tendências de adoção”, existe uma série de passos para um ativo se tornar moeda mundial plena:

A tendência, seguindo o caminho dos ativos já usados como moeda, seria substituir, primeiro, parte do mercado do ouro; depois, paraísos fiscais e *offshores*; então, imóveis, ações e títulos como reserva de valor.

Os ativos que seguiram essa progressão evoluíram por séculos. Não sabemos se, no nosso tempo de vida, o bitcoin substituirá as moedas nacionais.

Se alguns governos fizerem reservas em bitcoin, nem que seja através de expropriação, desapropriação ou tributação, talvez algumas moedas nacionais sejam lastreadas em bitcoin e durem mais uma ou duas gerações.

Em um de seus interessantes *insights*, Robert Breedlove deixa claro como moedas que funcionam como reserva de valor modificam o comportamento dominante de seus usuários: o dinheiro capitalista do livre mercado (bitcoin e ouro) incentiva a economia, já que a escassez gera apreciação e atenua as distorções do mercado, assim moralizando-o; já a moeda socialista (moeda fiduciária) incentiva o endividamento, à medida que a inflação diminui os

encargos das dívidas reais. Por esse motivo, existe a tese de que o uso generalizado do Bitcoin provocará uma Revolução[201] ou Renascimento[202] moral, tecnológico e material.

Mircea Popescu[203], desde 2012, advoga o oposto: que Bitcoin é a coisa mais conservadora neste planeta desde Jesus — vez que vai restaurar Lei Natural, moralidade, propriedade, liberdade e instituições naturais, como expresso no meme “BITCOIN FIXES THIS". Cristo mudou o mundo, mas afirmou que não vinha mudar a Lei (Antigo Testamento), mas sim para fazê-la ser cumprida[204].

2.4 A computação quântica não destrói o Bitcoin? O Bitcoin não foi hackeado?

Não, o Bitcoin não foi hackeado, empresas que usam o bitcoin sim**.**

Computadores quânticos[205] são computadores que exploram a mecânica quântica para realizar certos cálculos muito mais rápido que os computadores tradicionais.

Na computação quântica, os algoritmos e *softwares* processam informações através de sistemas quânticos, como átomos, fótons ou partículas subatômicas. Computador quântico não é uma máquina que roda mais rápido as mesmas aplicações, ele apenas é um artefato capaz de "rodar" alguns algoritmos específicos.

Um computador quântico suficientemente potente causaria alguns problemas ao Bitcoin. Porém, cabe salientar que a computação quântica não é uma ameaça só ao sistema de criptografia do Bitcoin, mas a todos os sistemas computacionais no mundo que utilizam aparatos de criptografia semelhantes com criptografia de chave pública-privada derivada de curva elíptica: sistemas bancários e de autorização de disparos de armas atômicas, por exemplo, seriam alvos em muitos aspectos mais vulneráveis e lucrativos. Outro *honeypot* preferencial seriam as carteiras antigas de Satoshi Nakamoto (ainda em tecnologia mais vulnerável).

Um endereço de Bitcoin está protegido de computação quântica desde que nunca tenha sido gasto. Ou seja, nunca tenha sido revelada a chave pública, por isso, usar cada endereço apenas uma vez é considerado procedimento padrão. Um endereço é o *hash* de uma chave pública. A chave em si só é revelada quando há gasto daquele endereço (e não depósito).

No entanto, ainda há tempo para a mudança de todo o cenário da área de segurança criptográfica de chaves públicas, com o desenvolvimento dos protocolos de criptografias quânticas. Há algumas pesquisas acadêmicas em andamento sobre a criação de algoritmos de chave pública com segurança quântica com muitas das mesmas propriedades dos algoritmos de chave pública de hoje, mas isso é muito experimental.

Computadores quânticos funcionais podem levar algum tempo (algumas gerações), principalmente porque é provável que os primeiros computadores quânticos sejam extremamente lentos, mas práticos para realizações de projetos específicos. Os computadores convencionais são ainda muito

rápidos em diversas atividades de processamento de informações e podem realizar muitas ordens de magnitude a mais por segundo, porque vêm sendo aprimorados nos últimos 40 anos.

O ex-desenvolvedor do *Bitcoin Core* Peter Todd[206] esclarece que o computador quântico não pode resolver qualquer tipo de problema com tanta velocidade de processamento; mas consegue resolver problemas específicos com uma grande rapidez, pois foi projetado para realizar um tipo de função de forma específica.

Atacar chaves criptográficas do Bitcoin exigiria cerca de 1.500 *qubits*. Atualmente, o mundo não possui a tecnologia necessária para criar um computador quântico grande o suficiente para atacar a criptografia da rede Bitcoin[207]. Não se sabe com qual rapidez essa tecnologia avançará, o ECRYPT II[208] estima que as chaves *ECDSA (Elliptic Curve Digital Signature Algorithm)* de 256 bits do Bitcoin tendem a ser seguras até, pelo menos, 2030-2040.

O Bitcoin já possui alguma resistência quântica embutida que proporciona uma mitigação necessária. Se você usar apenas endereços Bitcoin uma vez, o que sempre foi a prática recomendada, sua chave pública *ECDSA* só será revelada quando você gastar bitcoins enviados para cada endereço.

Um computador quântico precisaria ser capaz de quebrar sua chave no curto espaço de tempo entre o momento em que sua transação é enviada pela primeira vez e quando ela entra em um bloco. Entretanto, precisar-se-iam de décadas para que um computador quântico quebrasse uma chave criptográfica de Bitcoin, que, com as melhores práticas, só ficaria vulnerável por minutos.

Em outras palavras, segundo os *experts*, os medos sobre a computação quântica são exagerados e, apesar dos avanços nesta área, os engenheiros e cientistas ainda não sabem como criar um computador quântico suficientemente complexo a ponto de *hackear* o Bitcoin. Além disso, no dia em que essa missão for cumprida, deve ser adotado novo esquema criptográfico; e, antes de as carteiras mais recentes serem atacadas, as carteiras antigas e demais *honey pots* servirão de "canário na mina[209]".

Por fim, é útil lembrar que a ameaça da computação quântica já está sendo enfrentada com o desenvolvimento de provas de trabalho *quantum resistants*. Quando surgir uma máquina capaz de quebrar o *Proof of Work* da

Blockchain, basta aplicar rapidamente um *fork* para mudar essa prova de trabalho.

Em suma, computação quântica: a) está tão próxima quanto fusão nuclear (ou seja, possível em laboratório ou simulações, mas pode levar décadas ou gerações para aplicações comerciais); b) afetaria mais bancos e sistemas de defesa e infraestrutura (por serem maiores *honeypots* e mais vulneráveis) que o Bitcoin, "não preciso correr mais que o leão, preciso correr mais que você"; c) afetaria primeiro o milhão de bitcoins atribuídos a Satoshi em endereços antigos (e milhares de BTCs em endereços usados) e eles não ligam, temos canários na mina; e, d) poderia deixar de ser uma ameaça ao Bitcoin com atualização, já que é um software.

2.5 Quando eu morrer, para onde irão meus bitcoins?

Um caso seminal de como preocupações sucessórias com bitcoin se tornam práticas foi o de Hal Finney[210].

Quando bitcoins são enviados para endereços que não têm chaves privadas conhecidas (ou quando as chaves privadas para acessar saldos de endereços são perdidas), essas unidades passam a estar "perdidas". São como o ouro no fundo do mar, talvez um dia haja tecnologia para recuperá-los, talvez não.

Há diversas estimativas forenses[211] indicando entre 2,8 e 3,8 milhões de *tokens* perdidos (inacessíveis, provavelmente para sempre), aumentando a escassez e o valor das demais unidades.

Respondendo à questão, se você morrer, os bitcoins vão para onde você quiser, algumas possibilidades básicas podem ser enumeradas:

a) podem não ir para ninguém, enriquecendo o resto da comunidade, se você não deixar informações de como recuperar suas chaves privadas e senha, como único ativo que pode levar consigo para o túmulo;

b) podem ir para seus sucessores, legalmente, como qualquer saldo bancário, se tiver depositado em plataforma com *KYC – know your customer* (como walltime.info);

c) se a chave privada estiver impressa em papel, sem estar criptografada, quem tiver a posse material do papel passará a ser o proprietário dos bitcoins;

d) se estiver impressa em *paper wallet* criptografada, os bitcoins só serão acessados por quem detiver a chave e a senha (por isso, alguns *bitcoiners* informam aos sucessores como descobrir a senha e a chave, ou dão a senha a algumas pessoas e o acesso às chaves a outras);
e) se baixaram *wallet* no celular, ao recuperar o aparelho com senha, recuperam-se os bitcoins; ou
f) se for encontrada *hardware wallet*, quem souber a senha e tiver posse do aparelho poderá acessar os bitcoins.

Ou seja, Bitcoin dá a liberdade de planejar a sua sucessão mesmo fora dos limites legais de disposição. Se o usuário não revelar a potenciais sucessores que tem bitcoins, nem deixar nenhuma forma de eles descobrirem, é porque não quer que eles fiquem com nada.

Existe um dilema *(trade-off)* entre segurança e praticidade. Quanto mais acessíveis os bitcoins, menos seguros. Por isso, são mais confiáveis plataformas que mantêm quantidades maiores de saldos *off-line* (*cold wallet*) e menos *on-line* (*hot wallet*), sem contar os meios de aumentar segurança com *timelock* (saldos bloqueados por certo tempo) e *multisig* (exigência de múltiplas assinaturas para movimentação).

Exemplos extremos são o de quem concreta partes da *seed (mnemônicos)* em imóveis diferentes – exigindo tempo e acesso a ambos os imóveis para acessar os bitcoins; ou de quem concreta a *seed* (3 a 24 palavras, usualmente) criptografada em sua casa, informando pessoas de sua confiança que não têm acesso à *seed* a senha para descriptografar tal sequência.

Esquemas de *multisig* que exigem 4 ou 5 assinaturas de um total de 7 são usuais e permitem à família ou à sociedade empresarial continuar tendo controle dos bitcoins por maioria, mesmo com morte ou dissidência simultânea de 2 ou 3 atores (embora contenha risco no cenário de morte simultânea da maioria das partes, o que também pode ser mitigado pelo *backup* físico de suas chaves, nem que seja em cofre ou concretado em sua casa).

Uma simplificação da solução *multisig* é o *"Shamir's Secret Sharing scheme"*, disponível até mesmo em hardware *wallets* mais modernas.

Shamir Scheme permite que a maioria das pessoas que possuem partes da senha acessem o total dos saldos, sejam conjuntos de 2 de 3, 3 de 5 ou 4 de

7.

Assim, se você der uma senha dessas a sua mãe, uma a sua esposa e uma a seu testamenteiro, seriam necessários 2 desses 3 para sacar o saldo — não havendo perda mesmo com mortes simultâneas sua e de mais um deles.

Segregar diferentes *passphrases*[212] para saldos que queira deixar para cada sucessores é uma alternativa mais segura quanto a oportunismo, porém com mais risco de bitcoins serem perdidos em caso de mortes simultâneas. As palavras (*seed*) poderiam estar em local conhecido por todos os sucessores — em cofre ou concretada — e a respectiva *passphrase* seria entregue a cada um deles – o que pode ocorrer até após sua morte, automaticamente por *e-mail*.

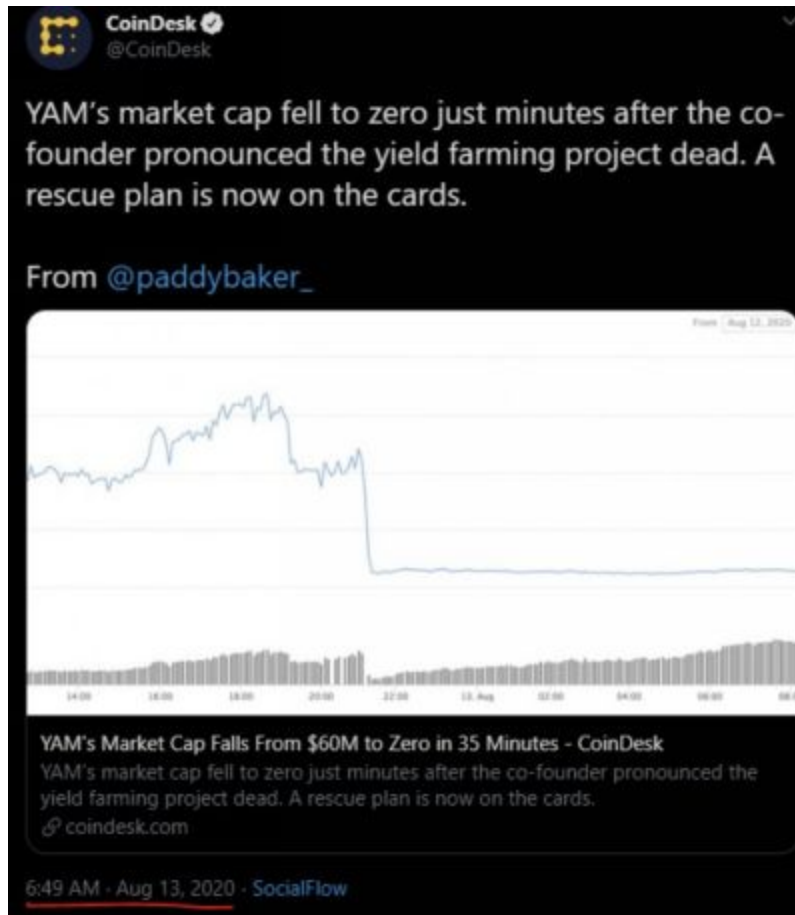
Nesse caso, a ferramenta sucessória útil é a função *"Dead man`s switch*", disponível desde 2013 gratuitamente no *Gmail* ou *"final message service"* (https://finalmessage.io/) que permite automatizar uma mensagem para alguém de sua confiança, que só é enviada após certo período de inatividade.

A mensagem final também pode ser *multisig* (multi assinaturas), forçando consenso entre sucessores para saque (total ou parcial). Há solução semelhante na rede *Lightning Network*[213].

Em resumo, ativando essa opção, são enviadas automaticamente mensagens por *e-mail* quando a conta atingir certo tempo de inatividade. Desta maneira, pode expressar suas últimas vontades, dando as instruções a seus sucessores de como acessar seus ativos — informando senhas e saldos (ou onde encontra-los) apenas para os beneficiários, sejam herdeiros ou legatários.

É vital lembrar que pode ser disparado antes de sua morte — caso fique a deriva, preso, hospitalizado, em cativeiro ou por qualquer outro motivo sem acesso à conta.

Até o desenvolvimento do Bitcoin não existia bem que não pudesse ser tomado à força, nem ativo cujo titular pudesse garantir que não fosse adquirido por ninguém após sua morte. Por isso, as nuvens mudaram o jogo, a criptografia é uma arma de guerra desde sua criação. Seu uso, nesse caso, inviabiliza a vitória por pura violência e força bruta.

2.6 Era vantagem comprar no início, não agora! Não seria melhor comprar a *shitcoin* que custa apenas 1 satoshi em vez de bitcoin? Ou comprar uma NFT que pode valer milhões em algumas semanas?

O valor de ativos que geram fluxos de caixa é calculado pelo fluxo de caixa esperado descontado pelos riscos e pela taxa de juro de mercado. O valor de *commodities* é normalmente correlacionado a sua escassez, como previsto no modelo do *stock to flow*[214].

Por isso, pretender ganhar mais comprando *altcoin* que bitcoin é o mesmo que pretender ganhar mais comprando cobre, alumínio ou ferro do que ouro. É possível aumentar seu patrimônio em ouro fazendo *trades* com prata, mas, no longo prazo, ao longo dos últimos 3.000 anos, quem manteve posições em prata por gerações seguidas invariavelmente perdeu poder de compra, medido em ouro[215].

A chance de uma *altcoin* substituir o bitcoin é a mesma de outro metal substituir o ouro.

A prata na Idade do Bronze valia 1/6 do grama do ouro, em Roma 1/12, nos padrões bimetálicos 1/16 e, desde a década de 1980, varia entre 1/35 e 1/125. Realmente, uma curva de baixa de mais de 3.000 anos. Estimativas de abundância de prata e ouro variam entre 1:16 e 1:18 (na crosta terrestre), entretanto, as relações de valor e escassez marginais não são lineares, mas exponenciais.

Uma comparação semelhante pode ser feita observando o índice de "dominância" do bitcoin (excluindo *stable coins* e *scams* com volumes e cotações manipuladas).

Altcoins são exponencialmente mais arriscadas que bitcoin e a maioria delas "virou pó" ou tende a virar após os controladores venderem o suficiente de suas posições.

Entre maximalistas, é crescente o entendimento que *altcoins* eram necessárias no início como *test nets (redes para testes de inovações) ou* camadas alternativas para envio de valores quando *fees* estivessem altas, porém, com soluções *offchain*, 2ª camada e *sidechains*, essa demanda não existiria mais e as *altcoins* seriam hoje apenas ataques de engenharia social contra o bitcoin (ou, mais especificamente, contra detentores de BTC sem estrutura para mantê-los). A única função intacta das *altcoins* é a de redundância, de manter sistemas ativos caso o Bitcoin pare de funcionar, por qualquer motivo e para testar conceitos em redes de menor valor.

De fato, há muitos fatos fundamentando alegações de que criadores em série de dezenas de *shitcoins* acumulam bilhões de dólares em *assets* sem investir nada além de promessas.

Evidências de golpes na criação de novas moedas são: adoção de *Proof of Stake* — esquema para remunerar quem já possui saldos; subsídio para desenvolvimento (vinculação de novas moedas para projetos que seriam aprovados por maioria, que são os próprios fundadores); e, *pre-mine*, ou seja remuneração em milhares de *tokens* pela “ideia” de criar a moeda[216].[217]

Grande parte das pessoas que ganham na loteria terminam piores do que se não tivessem ganhado. Perdem sua família, emprego, desperdiçam o prêmio e, no final, terminam mais pobres do que eram.[218]

Ter bitcoin é ganhar na loteria aos poucos. Só que a maioria das pessoas que obtêm grandes valorizações, por ausência de estrutura mental, emocional e familiar, perde tudo – seja com meretrizes, cocaína e luxos absurdos, seja vendendo tudo para recomprar mais barato depois (confirmando que, em geral, depois é nunca); ou mesmo comprando *shitcoins* para “aumentar o número de bitcoins”.

A maioria das *shitcoins* já viraram pó. Mais de 90% dos *forks* do bitcoin morreram, ninguém minera e nem há mercado para negociar esse *tokens*.

Esses golpes geram lucro aos seus criadores (principalmente por pré-mineração) e às corretoras (tanto em *fees* quanto cobrando para listar as *shitcoins*), invariavelmente. Alguns especuladores também lucram esperando comprar para vender “quando subir”, porém, eventualmente não sobe mais e os últimos a adquirir perdem tudo. É um jogo de soma negativa, mais riqueza é perdida que produzida – e a maioria absoluta dessa riqueza é capturada pelos golpistas e *exchanges* (*shitcoin casinos*), “a casa nunca perde”.

Quando alguém disser que ganhou dinheiro com ether, doge, shiba ou ripple – lembre-se que muita gente também ganhou com Telexfree, BBOM, Atlas Quantum, GBB, Minerworld, Ronaldinho 18K ou em "ações memes"[219].

2.6.1 Se *shitcoins* não são alternativas? Como diversificar?

Graças a mercados futuros de bitcoin, é possível fazer *"cash and carry"* travando ganhos acima de 30% a.a. em dólar nos mercados de alta[220]. Também se pode obter renda, em dólar ou ouro, com taxas de *funding* e *lending*[221] de *stables*. Infelizmente, não existe investimento em ambiente de juro real negativo, apenas *hedge* ou perda – fixa ou variável.[222]

Ler esse livro é diversificar: investir tempo em sua educação real. Alternativas de diversificação também são: investir em sua produtividade (em negócio próprio, em suas habilidades e *networking*) ou relações sólidas, como criar filhos dispostos e capazes de ser úteis.

Como Saylor deixa claro, quando você sabe qual a solução para um problema de engenharia, diversificar é "vender o vencedor, para comprar perdedores".

Na dúvida, pesquise no *ranking* dos bilionários quantos concentraram mais de 90% em apenas um ativo (Musk, Bezos, Gates…) e quantos diversificaram.

Seja grato:

A oportunidade de trocar "papel colorido lastreado em honestidade de político" por dinheiro de verdade logo vai acabar.

Quem veio na 1ª onda pôde ter milhares; na 2ª, centenas; na 3ª, dezenas; e na 4ª vão ser unidades ou mesmo frações.

Muita gente perdeu mais de 90% de sua riqueza investindo em *shitcoins* ou confiando em desconhecidos para fazer a custódia de suas moedas. Esteja aberto a aproveitar a oportunidade que você tem, ou a desperdiçará e lembre-se: *not your keys, not your coins*.

Sem gratidão você não recebe nada. Para receber algo de valor precisa estar aberto a aceitar. Para estar aberto precisa reconhecer o valor do que vai receber e como uma graça a oportunidade. Esse é um dos "fatores bilionários" identificados por Napoleon Hill[223].

Com *fiat*, a volatilidade é zero e há certeza de perda de poder de compra. No Bitcoin, a volatilidade é alta, perdas acima de 30% são comuns até em mercados altistas (*bull markets*) e de até 90% na baixa (*bear market*). Entretanto, seu retorno médio na década é superior a triplicar a cada ano (200% a.a.), em dólar. Prefere volatilidade ou certeza de perda?

O maior legado não é material.

As coisas mais baratas são pagas em *fiat* ou dinheiro. As coisas realmente valiosas são pagas com seu tempo de vida, honra, saúde ou oportunidade – e é de natureza moral, emocional, espiritual e educacional. Não existe almoço grátis.

Mais riqueza foi criada nos últimos 20 anos que nos 20.000 anteriores ao século XX, entretanto, se a tecnologia moderna não estiver mais disponível, 80% da população não terá como se alimentar em menos de uma semana, morrem de fome. Quanto mais complexos os sistemas, mais frágeis.

Ninguém vive de riqueza acumulada para sempre, você tem que se preocupar em transformar seus filhos em pessoas capazes de multiplicar e gerar riqueza – materiais ou não.

O comunismo é a escravidão suprema e para ser escravo é essencial que não tenha família, Deus ou legados – isso que vai acontecer se falharmos. Se você tem a Deus, família ou sabe de onde veio, não é escravizado. Como muito bem explicou Fernando Pessoa há quase 100 anos[224]:

Se o que há de lixo moral e mental em todos os cérebros pudesse ser varrido e reunido, e com ele se formar uma figura gigantesca, tal seria a figura do comunismo, inimigo supremo da liberdade e da humanidade, como o é tudo quanto dorme nos baixos instintos que se escondem em cada um de nós. O comunismo não é uma doutrina porque é uma antidoutrina, ou uma contradoutrina. Tudo quanto o homem tem conquistado, até hoje, de espiritualidade moral e mental — isto é de civilização e de cultura —, tudo isso ele inverte para formar a doutrina que não tem.

Dada a inviabilidade dos Estados Sociais e a radicalização das "bolhas", não há possibilidade de acordo: ou a humanidade será livre e próspera como ninguém nunca foi (se o totalitarismo for inviabilizado ou derrotado, com o extermínio dos criminosos pelos mercados de apostas descentralizadas de morte); ou, será escravizada e submissa de maneira sem precedentes, se o modelo chinês for dominante, com monitoramento de cada palavra (dita, ouvida ou escrita) e sistemas de crédito social[225] e expurgos[226].

Seu tesouro está onde está o seu coração. Todos os dias renunciamos um pouco de nossa liberdade, cada opção é renunciar a todas as alternativas. Dinheiro é a forma de concentrar tempo, liberdade e esforço para conseguirmos a liberdade (em tempo livre, risco e esforço) de outras pessoas.

Vender bitcoin para realizar um sonho, melhorar sua saúde, obter independência financeira ou adquirir território soberano é totalmente compreensível. Contudo, até o final desse ciclo, com as plataformas de colateralizados contra carteiras diversificadas, nem isso será necessário.

Exemplos de pioneiros que moram na mesma casa e mantêm o mesmo padrão de vida são Nick Szabo e Laszlo[227] (que 10 anos depois da pizza de 10 mil bitcoins ainda morava na mesma casa).

Há dezenas de exemplos opostos: de gente que desperdiçou a riqueza com “lambos”, *NFTs*[228] (*uma forma quase tão boa de lavar dinheiro quanto o próprio mercado de arte*[229]), drogas, prostituição e ostentação absurda ou perdeu tudo com *shitcoins*, falsos *giveaways*, outros golpes. A ostentação é um dos sinais de ganho fácil e é típica dos piramideiros: *easy come, easy go.*

Uma das formas atuais de ostentação absurda é a aquisição de *NFTs* por valores milionários. *Tokens* não fungíveis foram concebidos[230] em 2012, “*colored coins*”; e, existem exemplos desde 2014. Podem ser úteis como prova pública de certificado de autenticidade ou propriedade.

Se um artista ou casa de leilão envia *NFT* comprovando que detentor de certo endereço é o comprador legitimo da obra X, ele poderia transferir publicamente essa propriedade sem revelar quem adquiriu abertamente (apenas seu endereço). São análogos a *NFTs*, os elementos de jogos (personagens, *skins* e elementos particulares ou genéricos, ou fungíveis, seriam *"drops")* em ambientes fechados centralizados. Também podem ser registrados em *sidechain,* como na *Liquid*[231].

Em suma:

a) Mais de 90% das *altcoins* são golpes e mais de 99% incapazes de entregar o que prometem. Você conhece quem está à frente do projeto? Estudou o *whitepaper*? Grande parte dos projetos são cópia da cópia do *paper* principal ou copiam melhorias propostas nos *BIPs*;

b) Existem vantagens em todas essas experiências com *altcoins*. Porém, há também choro e ranger de dentes, a cada ciclo;

c) O tempo e esforço necessários para acompanhar *shitcoins* é enormemente maior do que fazer o mesmo com o Bitcoin.

2.6.2 Melhores práticas de segurança para custódia própria de bitcoin:

Sua *OPSEC* (segurança operacional) sempre vai variar com sua tolerância a riscos e com o ambiente. A Internet não esquece nada. Uma foto de rosto pode identificar qualquer um. Perfis identificáveis em redes sociais ou mesmo registro de localização em eventos políticos podem resultar em expurgos e perseguição derivada da associação de *big tech* com governos totalitários. Dai a importância de Satoshi permanecer anônimo. Privacidade vai passar a ser mais valiosa que popularidade com o entendimento do poder do *big data*.

Para não ser vítima, leia e entenda as “seis leis de Maca para não ser roubado”[232]

Se sua *bag* for menos de 10% do seu patrimônio total, manter *hardware walle*t bem guardada com *seed (*com *passphrase)* em múltiplos imóveis (em caso de incêndio, por exemplo) ou em chapa de aço (como da *Stackbit*[233] ou *Seedplate* da *Coinkite*) em lugar seguro é, normalmente, o suficiente.

Se seu investimento em BTC for para as futuras gerações; ou, for mais de 2 ou 3 anos de sua renda; ou, mais de 50% de seu patrimônio, manter em *hardware* mais de 10% a 20% dos saldos é loucura, mesmo com *plausible deniability*[234].

Melhor prática, no caso, é deixar os *hardwares* todos resetados – até para pensar bem antes de mover e mandar para Elon Musk (em falso *giveaway*[235]); ou, pior, dar a senha sob ameaça, coação e constrangimento[236], *"Wrench attack*”[237], situação que, ganhando tempo,

pode até mesmo conseguir janela de oportunidade para matar sequestradores – já que sabe que se eles te matarem, perdem a possibilidade de acesso aos bitcoins.

Para grandes quantias, ideal é deixar de 60% a 90% em cold – pode ser *multisig* tipo *"shamir's secret sharing scheme"*, em que 3 de 5 partes têm que concordar para mover (até mandando para os parentes as palavras em arquivo criptografado por *email*); pode ser uma *paper* e uma chapa de aço (com *passphrase* e em locais diferentes). Mais simples, se não tiver um monte de herdeiros, é dar a um parente cópia das palavras e a outra pessoa (ou pessoas partes) a *passphrase*.

Por exemplo: *seed* para a mãe ou pai – e uma *passphrase* para esposa para acessar metade e uma *passphrase* para padrinho para acessar metade para dar aos filhos adultos ou aos pais se estiverem em real dificuldade. Se sua mãe achar que sua mulher te matou, ela impede perpetuamente que a cônjuge acesse os bitcoins – mas ambas podem legar as referidas chaves a netos, após a morte da outra. Se sua mãe, esposa e compadre entrarem em conluio para te roubar, realmente, bitcoin não vai ser sua maior preocupação.

Outro bom exemplo: viúvo com 5 filhos – uma *seed* no cofre ou concretada em casa em lugar que todos os 5 saibam onde está (mas que não tenham como acessar sem chamar atenção, fazer barulho e ter trabalho) e o legado de cada um é acessado com uma *passphrase* que já deu previamente a cada um deles. O máximo que cada filho poderia roubar é o saldo que já estava reservado para ele – e seria publicamente sabido.

Se você ainda quiser manter satoshis no celular para fazer pequenos pagamentos pela LN, tudo bem, só deixe a quantidade de riqueza que você sairia no bolso na rua desarmado no centro de uma cidade grande de Banânia.

Se você ainda quiser manter saldos em plataformas para fazer "*trade*", capitalizar ou gestão, pelo menos não deixe na mesma plataforma mais de 2 a 3 anos de sua renda nem 10% de seu patrimônio total – e com *whitelist* para os bandidos terem que dominar você e te manter vivo por 14 a 16 dias para poder subtrair o saldo lá.

A tendência é que os esquemas de "falsos *giveaways*", "falsas *wallets*" e "trade de *shitcoins*" sejam logo substituídos pelo *"wrench attack (trench hack)*" — alguém te dominar metendo furadeira, porrada, choque ou mutilando você e sua família para que entregue suas chaves.

Se nem você puder mover 90% a 95% dos seus BTC sem sair de casa ou esperar 14 a 18 dias, você e toda a comunidade estarão mais seguros inviabilizando esse tipo de golpe — e o parente que sair vivo ainda vai ter 10x a 20x mais grana que os bandidos para caçá-los e colocar suas cabeças a prêmio. Se a maioria fizer isso, resta inviabilizado esse tipo de crime.

2.7 Evolução das narrativas

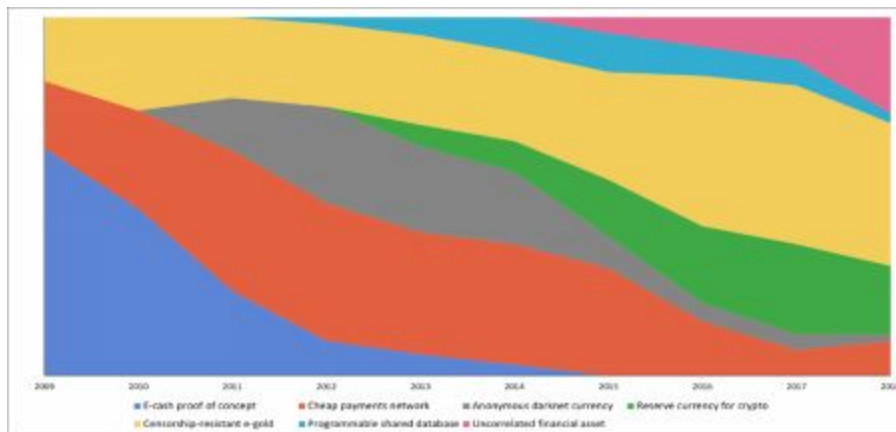
Nic Carter e Hasu mostraram em seus estudos[238] como as narrativas do Bitcoin mudaram ao longo do tempo. A discussão mais recorrente e antiga dentro da comunidade é sobre qual o principal propósito ao qual o Bitcoin deve servir: dada a sua multiplicidade de funções (meio de pagamento, reserva de valor e base de registros públicos incensuráveis) e o fato de a rede evoluir, tanto em *software* quanto em *hardware*, suas principais funções e utilidades são objeto de debate com narrativas novas a cada era.

Como se pode perceber, as visões do Bitcoin não são estáticas, logo as narrativas no universo do Bitcoin surgem, portanto, de grupos que mantêm visões muito particulares sobre o protocolo, acarretando muitas vezes “atritos” quando essas visões não são conciliáveis. Por isso, todo o aparato de consenso da rede faz com que todos os participantes contribuam para a melhor manutenção do funcionamento do protocolo.

Satoshi Nakamoto não quis ser visto como um único ponto de falha que poderia degradar bastante a segurança da rede e se ausentou em 2011. A causa provável de seu desaparecimento dos fóruns de discussões não foi explicada por Satoshi. Mas o fato de o criador se retirar não exercendo autoridade em decisões, não recebendo subsídio de desenvolvimento, nem se beneficiando financeiramente de ser pioneiro (deixando moedas paradas até hoje), é o que se denomina “concepção sem pecado”. Uma das características do Bitcoin que não há como ser facilmente repetida.

Podemos considerar que o Bitcoin ainda é um ativo em descoberta. O gráfico (*Visions of Bitcoin*)[239] a seguir mostra a influência das sete narrativas mais influentes do Bitcoin:

1. Prova de conceito de dinheiro eletrônico (azul);

2. Rede de pagamentos ponta a ponta de baixo custo (vermelha);
3. Ouro digital resistente à censura (amarela);
4. Moeda anônima da *darknet* (cinza);
5. Moeda de reserva para o ecossistema cripto (verde);
6. Banco de dados programável distribuído (azul claro);
7. Ativo financeiro descorrelacionado (rosa).

Saylor[240] defende o Bitcoin como solução de engenharia para o problema da reserva e transporte de valor - em uma argumentação muito próxima de Popescu de que “Bitcoin é pura matemática”.

Em resumo, Bitcoin representa "muitas coisas para muitas pessoas”: investimento especulativo; reserva de valor; meio de registro de outros ativos; meio para exercício da desobediência e desinvestimento do *legacy;* dinheiro programável; banco de dados descentralizado programável; plataforma para comunicação incensurável.

> Bitcoin is fate. It operates completely outside of any human agency, even if it was (possibly) some people that created it. For all you know about who Nakamoto was … Bitcoin might as well have created itself. The way fate works is quite simple: do the right thing and you're part of it. Do the wrong thing(s) and you're in the dark, huddling corners, wondering what went wrong and why does "the mainstream" oppress you so. And that "right thing" scarcely ever has anything to do with what "the community" thinks, wants or imagines. It is, after all, math.
>
> Mircea Popescu

3 (Why?) - Por que Bitcoin?

A necessidade vital de um dinheiro privado superior para limitar os abusos estatais foi prevista desde Rothbard e Hayek[241] em *O que o governo fez com nosso dinheiro* e *Desestatização do Dinheiro*:

> Acredito que nunca teremos um bom dinheiro novamente antes de tirar a coisa das mãos do governo, não podemos tirá-lo violentamente das mãos do governo, tudo o que podemos fazer é, por algum meio indireto, introduzir algo que eles não podem parar.

Hayek já tinha previsto que o Estado perderia o monopólio de emissão de moeda para alternativas privadas superiores. Friedman, em 1999, previu[242] objetivamente que uma "moeda digital que permita transações tão anônimas quanto as efetuadas em dinheiro" seria criada como o "dinheiro da Internet" logo que o problema do gasto duplo fosse resolvido — como Peter Thiel[243].

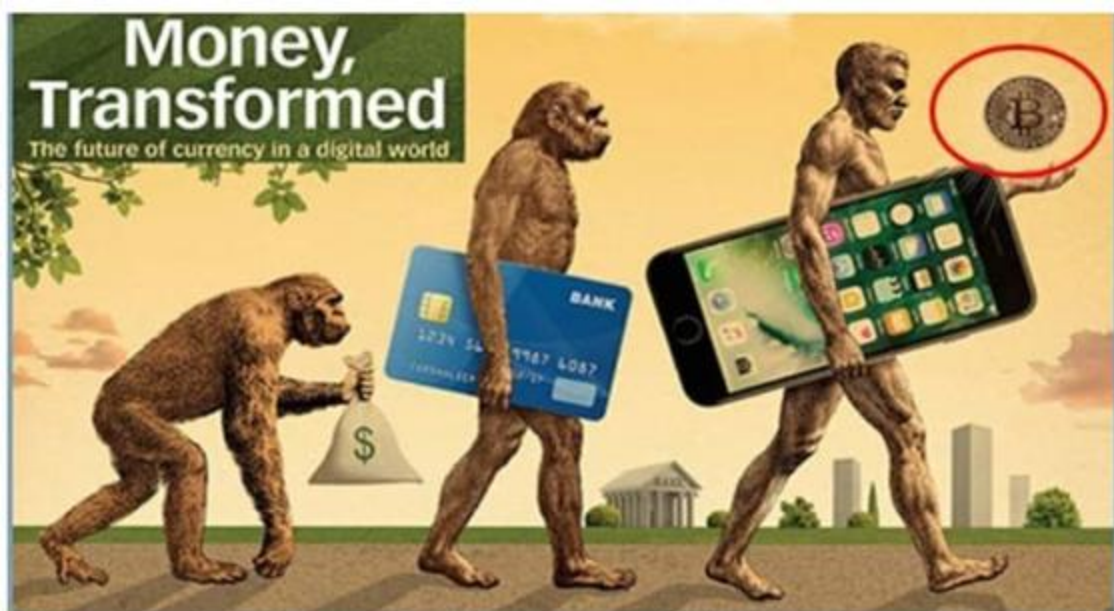
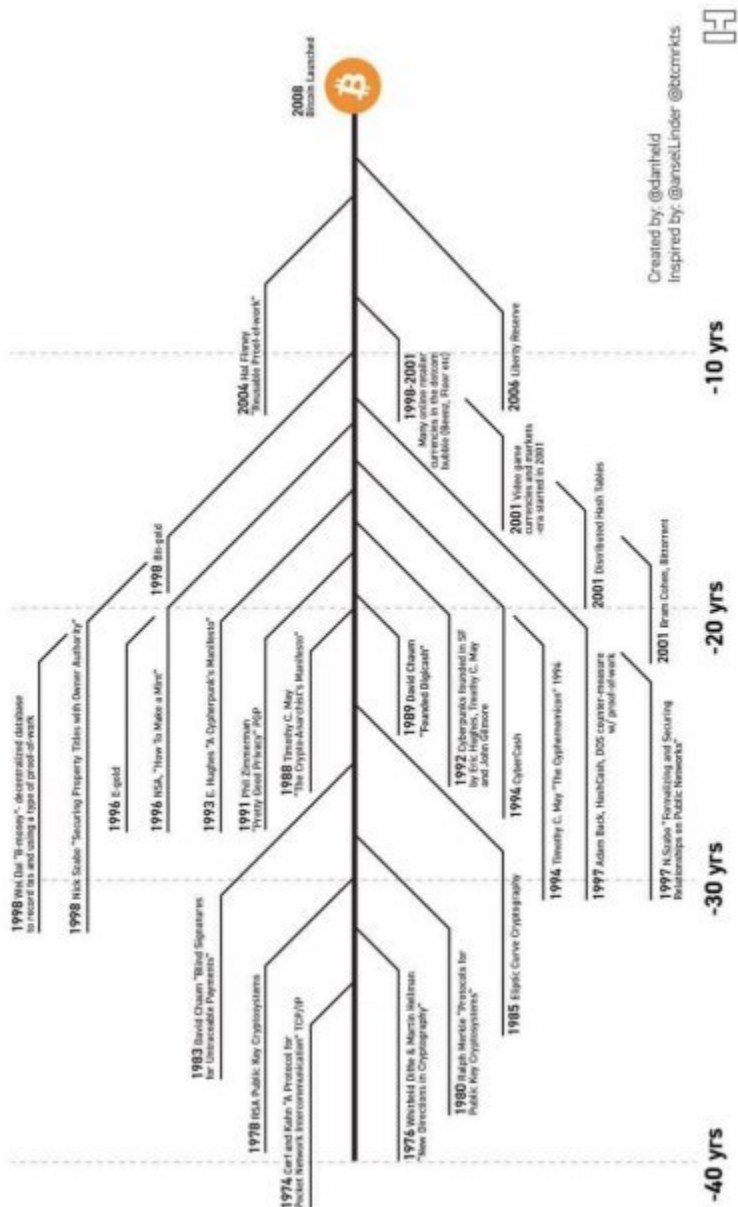
Satoshi Nakamoto resolveu o problema dos Generais Bizantinos[244] ou problema de ataque coordenado, por meio do desenvolvimento da primeira *Blockchain* viável (embora a expressão original tenha sido *timechain* em 2008).

O Bitcoin foi criado e obteve sucesso porque responde a uma demanda urgente da atualidade: um dinheiro imune a controle de capitais, expropriações e tributos involuntários, diluição por governos, e que é descentralizado, incensurável e programável.

Como Satoshi deixa claro em sua primeira mensagem no Bloco Gênese, foi o abuso do poder dos governos que os fez perder o monopólio de emissão das moedas – cada vez mais claro com a guerra ao dinheiro, os juros negativos e os *QE4ever* (alívios quantitativos perpétuos).

Satoshi Nakamoto, em seu artigo referência, reconhece as contribuições de autores e tentativas anteriores de criptomoedas e sistemas descentralizados[245] (*HashCash*, de Adam Back, e *B-Money*, de Wei Dai).

O Bitcoin não foi a primeira criptomoeda nem a primeira tentativa de sistema de pagamentos eletrônicos descentralizados, porém, foi a primeira a ter sucesso por conjugar soluções criadas até então, aprendendo com os erros das tentativas anteriores. Foi a solução necessária no momento certo.

O futuro da moeda em uma palavra: digital[246]

Linha cronológica dos predecessores do Bitcoin

ANO	SERVIÇOS/TECNOLOGIAS
1983	*eCash*
1993	*Hawthorne Exchange*
1994	*Magic Money*

1995	*Digicash/Cyberbucks*
1996	*e-gold*
1998	*BitGold*
2001	*Liberty Reserve*
2008	*Bitcoin*

3.1 Uma breve história monetária

O porquê do Bitcoin é a História da moeda[247]: a falência de todos os sistemas monetários já tentados, sejam *fiat* ou *gold standard,* falhos em honrar promessas e manter valor no longo prazo, por motivações oportunistas intrínsecas.

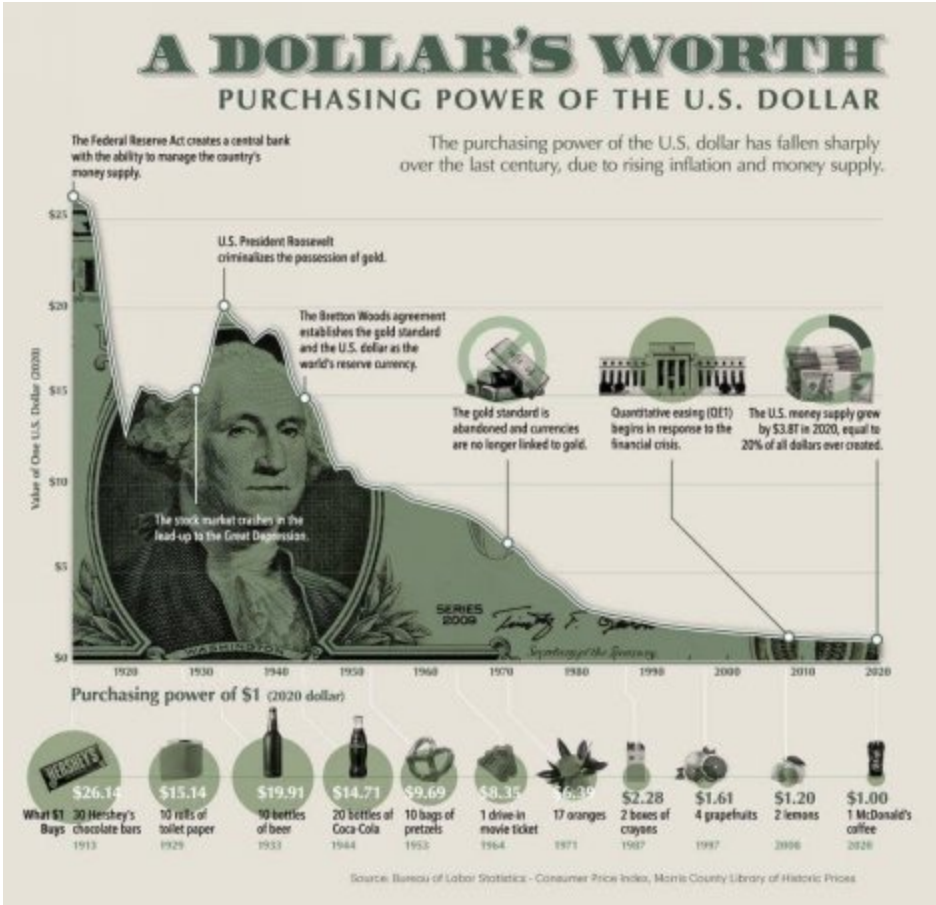
A moeda é adotada, mesmo em sistemas falhos, porque soluciona o problema da dupla coincidência de desejos[248] entre pessoas que desejam trocar entre si suas posses. Riqueza é subjetiva e criada do trabalho ou comércio[249]. Então, é possível que todos estejam em melhor condição meramente redistribuindo bens para os entes que os valorizem mais. Assim, há mais trocas quando existe moeda em vez de mera permuta direta de bens (que podem não ser divisíveis, duráveis nem transportáveis).

O fim do Acordo de Bretton Woods, em 1971, ou seja, o abandono do padrão ouro (*gold window*) tornou quase todas as moedas do mundo totalmente fiduciárias *(fiat money).*

Uma vez que os governos puderam imprimir moeda de maneira ilimitada, a moralidade política entrou em decomposição, tanto na distribuição do *welfare*[250] quanto na ampliação brutal de poderes dos governos, como no *warfare* (estatização da guerra).

Os resultados desses processos são mais guerras, mais gastos fora das capacidades arrecadatórias diretas dos governos e mais corrupção — uma vez que motivações oportunistas e consumistas a entes privados passam a ser dominantes: dos beneficiários de *welfare* que desistem de trabalhar até os bilionários que se dedicam apenas à captura administrativa[251]. Do indigente ao bilionário só vale a pena o oportunismo.

Prova disso é que os maiores bilionários do mundo são cantilionários (metacapitalistas), pessoas que gozam o privilégio de receber as novas moedas primeiro, por ter comprado influência em governos, por meio de financiamento estatal, sejam subsídios, contratos públicos ou mesmo compra dos títulos de suas empresas em *bailouts* (como denunciado no bloco gênese).

Declínio do Poder de Compra do Dólar *versus* Real

Em 1933[252], a moeda de 20 dólares (USD ou US$) era feita de uma onça de ouro (XAU); em 2020, 1 XAU chegou a custar mais de 2000 USD. Quem guardou dólar no colchão perdeu mais de 99% (em ouro) em menos de 90 anos – essa é a demonstração da senhoriagem e expropriação por inflação em um país "modelo".

De 1839 a 1933, havia moedas circulando com 33 gramas (mais de 90% de ouro) com valor nominal de 20 USD. Em 1933, o governo desapropriou o ouro privado pagando 20 USD e logo depois tabelando em 35 USD/OZ. Relação de escassez e valor é inexorável:

BTC > XAU >> XAG >> USD >> BRL >>ARS >> VES

Agora é a vez de mostrar como a República no Brasil[253] era desmoralizada desde o início: 2000 réis de 1912 com 20g (90% prata) era equivalente a 18 gramas de prata; e 2000 réis de 1924 com 8g (50% prata) era equivalente a 4g (4/18 = 1/4.5). Em 12 anos, os réis foram diluídos em quase 5x — isso porque ainda existia lastro em metal.

Atualmente, a diluição é ainda maior e os juros negativos destroem qualquer patrimônio do poupador honesto no *legacy*. Se você tem investimento em bolsa bolivariana, como a B3, pergunte a si mesmo: quantas empresas abertas existiam em Banânia (ou outro Estado de Exceção bolivariano) em 1924? E em 1984? E, entre essas, quantas não viraram pó?

A diluição do valor da moeda leva à diluição da moral, pública e privada: menos motivação para trabalho, esforço, poupança, investimento e

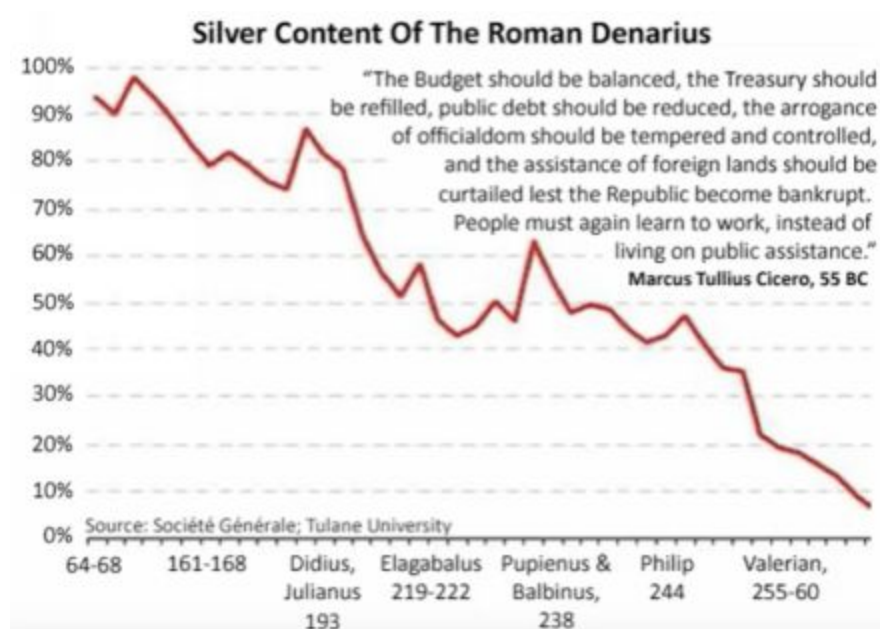
cooperação e mais motivação para vagabundagem, consumo, parasitagem, vitimismo e oportunismo.

Por isso, se o Bitcoin sobreviver mais 10 anos, haverá um Renascimento moral, material e tecnológico.

O ápice das distorções veio, a partir da crise do *subprime* nos EUA em 2008, com as políticas de alívios quantitativos (QE, *quantitative easing*, eufemismo para "criar dinheiro do nada" em quantidades sem precedentes), que impuseram tabelamento no preço mais importante na sociedade: o juro, preço da moeda.

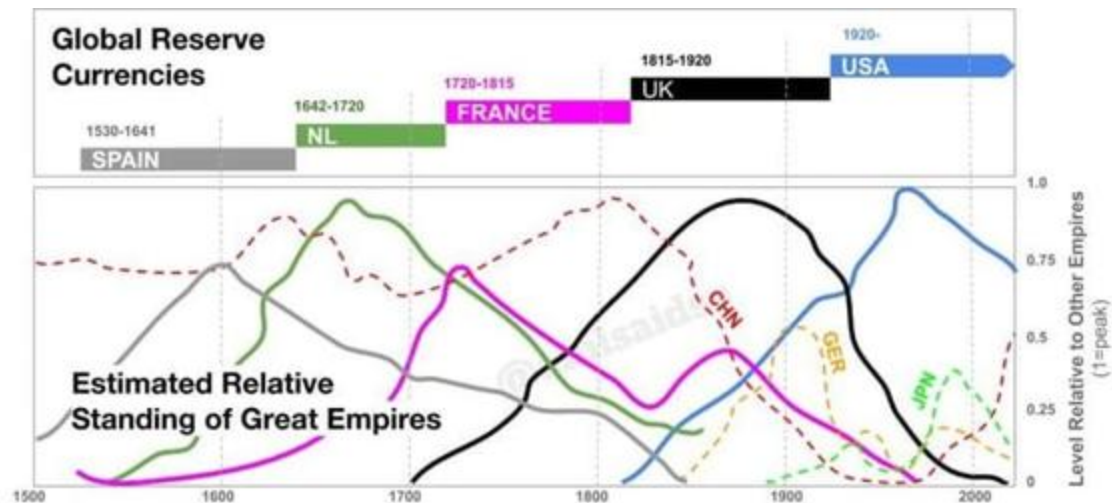
Em vez de permitir que empresas em crise quebrassem, para que a inovação, o empreendedorismo e a destruição criativa atuassem como expurgo natural, os governos usaram (e continuam usando) quantidades brutais de dinheiro público para salvar bancos e empresas.

Essa atuação aumenta a desigualdade social (ao inflar o valor dos ativos), reduz o crescimento econômico (ao reduzir as motivações para poupança e trabalho) e produz as distorções que inviabilizam a continuidade dos Estados Sociais – como previsto em *O caminho da servidão*, de Hayek, desde 1944.

Como diversas civilizações, os romanos também destruíram seu império degradando sua moeda:

Domínio das moedas de reserva mundial[254]

HISTORY OF WORLD RESERVE CURRENCIES
GLOBAL
BUILD-UP PERIOD
??? YEARS – 2030 to 21??
7.0
911 TERRORIST ATTACKS & WAR ON TERROR
AMERICA
BUILD-UP PERIOD
110 YEARS – 1920 to 2030
6.0
BRITISH EAST INDIA COMPANY DECLINE, WW1, GREAT DEPRESSION & WW2
BRITAIN
BUILD-UP PERIOD
105 YEARS – 1815 to 1920
5.0
FRENCH REVOLUTION, NAPOLEONIC WARS
FRANCE
BUILD-UP PERIOD
95 YEARS – 1720 to 1815
4.0
WORLD WIDE HUMAN MORTALITY RATE
DUTCH EAST INDIA COMPANY DECLINE, ANGLO-DUTCH WARS
NETHERLANDS
BUILD-UP PERIOD
80 YEARS – 1640 to 1720
3.0
WORLD POPULATION (BILLIONS)
DUTCH OCCUPATION, CATALAN REVOLT, FALL OF THE IBERIAN UNION, THIRTY YEARS' WAR
SPAIN
BUILD-UP PERIOD
110 YEARS – 1530 to 1640
2.0
EXPANSION OF USD LIQUIDITY AS
INTERNATIONAL RESERVE ASSET
FIRST INDUSTRIAL REVOLUTION
PORTUGUESE SUCCESSION CRISIS, IBERIAN UNION
PORTUGAL
80 YEARS – 1450 to 1530
1.0
SECOND INDUSTRIAL REVOLUTION
WORLDS FIRST CENTRAL BANK ESTABLISHED IN 1609 – BANK OF AMSTERDAM
1400
1450
1500
1550
1600
1650
1700
1750
1800
1850
1900
1950
2000
2050
2100

Visualizing Interest Rates Throughout History
Dutch Perpetual Bonds
The oldest perpetual bond still generating payments is dated 1624.
Genoa Republic
4-5yr Lending Rate
1555, 1566
9.0%
1.1%
1619
U.K. 3%
Perpetual Bond
U.S. 10-year Treasury
14.2%
1974
13.9%
1981
2.2%
1897
1.9%
1941
Race to the Bottom?
Since the 1980s, interest rates set by government debt have been rapidly declining, while the global economy has rapidly expanded.
Financial Crisis
Eurozone Crisis
Financial crises have driven interest rates to just above zero in order to spur spending and investment.
Federal Funds
Official Target Rate
Bank of England
Base Lending Rate
Sources: Sidney Homer and Richard Sylla - A History of Interest Rates, Federal Reserve, Bank of England

Dados de 500 anos das moedas de reserva global –
Posição relativa dos grandes impérios[255]

Os subsequentes *QE*s buscaram estimular a economia baixando os juros artificialmente, emitindo moeda do nada *(out of thin air*) para que os Bancos Centrais comprassem títulos soberanos (do próprio governo) e até mesmo ativos privados de qualidade no mínimo questionável, tendo atuado como investidores de última instância. Atualmente, 70% dos *ETFs* (fundos de índices, que compram ações e títulos) no Japão pertencem a entes públicos[256], e o BC Suíço[257] é um dos principais acionistas da *Exxon*, *Microsoft*, *Google*, *Facebook* e *Apple*.

O desempenho desse papel extremamente atípico por parte dos Bancos Centrais explode as suas bases monetárias e endividamento, comprometendo sua idoneidade regulatória (BCs são “donos” das entidades a que pretendem fiscalizar) e distorcendo motivações, ao superestimular a ociosidade e o consumismo e ao reprimir a poupança e a produção orientada às reais necessidades do mercado.

Diversas empresas nunca apresentaram lucros por mais de uma década, como *Amazon, Netflix* e *Uber* – sem contar as obras faraônicas e sem qualquer cabimento financeiro do “milagre chinês” (metade do crescimento do mundo desde 2008 ocorreu na China, onde abundam dezenas de milhões de residências vazias e milhares de obras[258] e empresas zumbis). Tudo isso só existiu graças a essas distorções decorrentes do juro negativo e dos “alívios quantitativos”.

Observe, nesta tabela de agosto de 2021, que as taxas de juros nominais tabeladas pelos Bancos Centrais, após o ajuste dos índices de inflação de preços ao consumidor (assumindo que são idôneos), resultam em taxas negativas e, quando positivas, situam-se muito próximas do zero:

Global Central Bank Policy Rates						
Country	Rate	Central Bank Rate (Today)	CPI YoY	Real Central Bank Rate	Last Move	Last Move Date
Switzerland	Target Rate	-0.75%	0.7%	-1.5%	Cut	Jan-15
Denmark	Deposit Rate	-0.60%	1.7%	-2.3%	Hike	Mar-20
Eurozone	Deposit Rate	-0.50%	2.2%	-2.7%	Cut	Sep-19
Japan	Policy Rate Bal	-0.10%	0.2%	-0.3%	Cut	Jan-16
Norway	Deposit Rate	0.00%	2.9%	-2.9%	Cut	May-20
Sweden	Repo Rate	0.00%	1.3%	-1.3%	Hike	Dec-19
Poland	Repo Rate	0.10%	4.4%	-4.3%	Cut	May-20
UK	Bank Rate	0.10%	2.5%	-2.4%	Cut	Mar-20
Australia	Cash Rate	0.10%	3.8%	-3.7%	Cut	Nov-20
US	Fed Funds	0.13%	5.4%	-5.3%	Cut	Mar-20
Canada	Overnight	0.25%	3.1%	-2.9%	Cut	Mar-20
Peru	Policy Rate	0.25%	3.8%	-3.6%	Cut	Apr-20
New Zealand	Cash Rate	0.25%	3.3%	-3.1%	Cut	Mar-20
South Korea	Repo Rate	0.50%	2.6%	-2.1%	Cut	May-20
Thailand	Policy Rate	0.50%	0.5%	0.1%	Cut	May-20
Czech Republic	Repo Rate	0.75%	2.8%	-2.1%	Hike	Aug-21
Chile	Base Rate	0.75%	3.8%	-3.1%	Hike	Jul-21
Hong Kong	Base Rate	0.86%	0.7%	0.2%	Cut	Mar-20
Saudi Arabia	Reverse Repo	1.00%	6.2%	-5.2%	Cut	Mar-20
Taiwan	Discount Rate	1.13%	2.0%	-0.8%	Cut	Mar-20
Malaysia	Policy Rate	1.75%	3.4%	-1.7%	Cut	Jul-20
Colombia	Repo Rate	1.75%	3.6%	-1.9%	Cut	Sep-20
Philippines	Key Policy Rate	2.00%	4.0%	-2.0%	Cut	Nov-20
South Africa	Repo Rate	3.50%	4.9%	-1.4%	Cut	Jul-20
Indonesia	Repo Rate	3.50%	1.5%	2.0%	Cut	Feb-21
China	Loan Prime Rate	3.85%	1.1%	2.8%	Cut	Apr-20
India	Repo Rate	4.00%	6.3%	-2.3%	Cut	May-20
Mexico	Overnight Rate	4.25%	5.9%	-1.6%	Hike	Jun-21
Brazil	Target Rate	5.25%	8.4%	-3.1%	Hike	Aug-21
Russia	Key Policy Rate	6.50%	6.5%	0.0%	Hike	Jul-21
Turkey	Repo Rate	19.00%	19.0%	0.1%	Hike	Mar-21

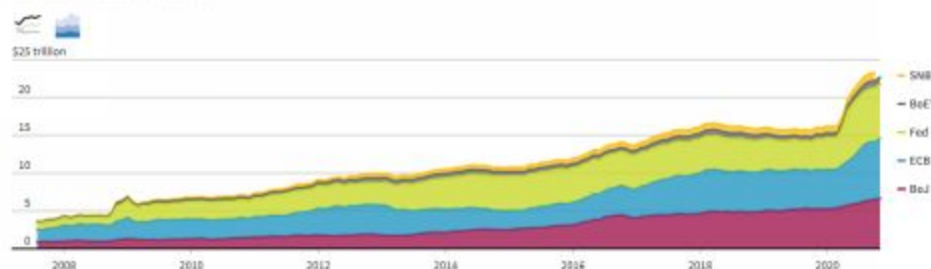
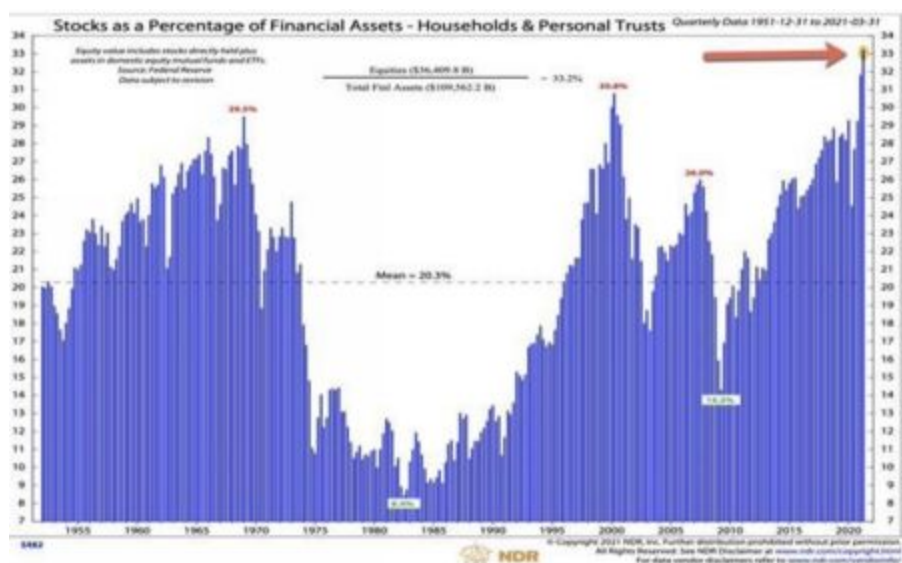
@CharlieBilello

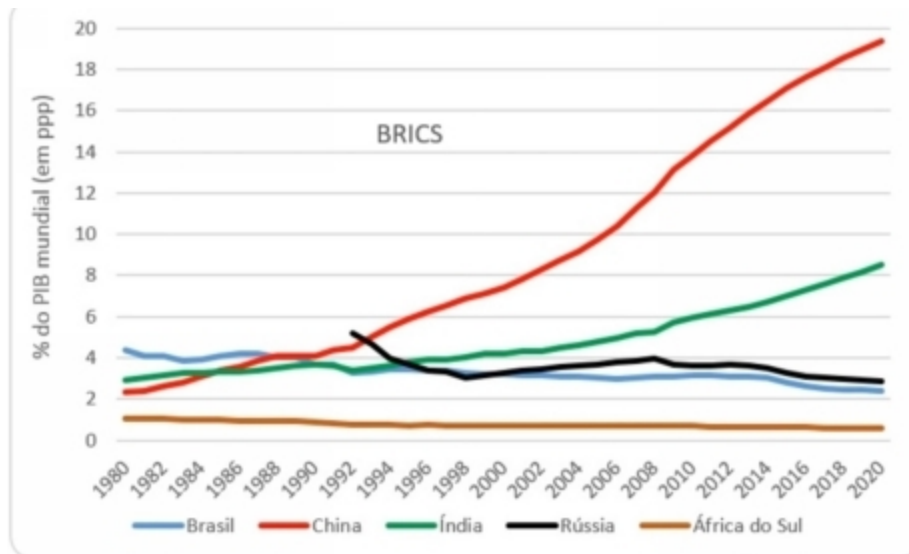
A história nos mostra que a corrupção dos sistemas monetários leva à decadência moral, colapso social e escravidão. A tentação de manipular dinheiro sempre se mostrou forte demais para a humanidade resistir.

@Breedlove22 *(Twitter)*

No mundo do dinheiro fiduciário, ter acesso às torneiras de dinheiro do banco central é mais importante do que atender clientes. As empresas que conseguem obter crédito com taxas de juros baixas terão uma vantagem persistente sobre os concorrentes que não conseguem. Os critérios para o sucesso no mercado tornam-se cada vez mais relacionados à capacidade de garantir financiamento a taxas de juros mais baixas do que à prestação de serviços à sociedade.

(O Padrão Bitcoin)

A expansão da estatização de ativos assusta[259]. Bancos centrais quintuplicaram ativos (estatização de mercados) em menos de 12 anos e hoje estatizaram mais de 50% do PIB dos seus respectivos países[260] (enriquecendo amigos do rei, multiplicando número de bilionários e explodindo desigualdade social):

Ações mais caras desde sempre

**Metade do crescimento mundial entre 2008 e 2019 foi na China
Quase tudo devido a juro negativo e tolerância aos crimes da ditadura:**

Fonte: Fundo Monetário Internacional (FMI) – visitado em 12/04/2016
(Nota: 2016 a 2020 = projeção) http://www.imf.org/external/datamapper/index.php

Ampliados diversas vezes os agregados monetários (quantidade de moeda) e os estoques de dívidas mundiais (públicas e privadas) e inflados os valores de ativos (imóveis, títulos e ações, por exemplo), dois cenários são resultantes: 1) a normalização dos juros acarretaria uma explosão no custo de endividamento dos Estados (já deficitários) e uma desvalorização brutal dos ativos (já que sua avaliação é, normalmente, feita por fluxo de caixa descontado por taxa de juro), resultando em colapso agudo das contas públicas e das moedas estatais; ou 2) a manutenção sistemática de juros negativos, com o empobrecimento também constante de quem investir no sistema sem ter acessos políticos para se beneficiar de captura administrativa, resultando no colapso crônico da poupança privada.

Conclui-se que o sistema financeiro convencional, *legacy*, tem seus dias contados até que ocorra uma correção que deve acabar ou tornar insignificantes a maioria das moedas, empresas e governos do presente – como asseveram Peter Schiff, Mike Maloney e Max Keiser ao afirmar que a próxima crise será maior que a de 2008, a de 1998 e até mesmo a de 1929.

Quem investiu na bolsa americana no topo de 1929 só se recuperou (ajustado pelo *CPI – consumer price index*) 52 anos depois[261]. Após 63 anos, quem investiu no topo ainda estava com ZERO GANHO e perda em

mais de 80% do tempo. Isso é a bolsa americana, onde há lei e governança para que mercados mobiliários sejam viáveis:

Em suma, é comprovada a perda das qualidades aristotélicas de dinheiro (capacidade de reserva de valor, fungibilidade, transportabilidade, divisibilidade e durabilidade) das moedas fiduciárias emitidas pelos governos, que só circulam devido ao curso forçado – ameaça violenta – até mesmo em decorrência de experimentos de demonetização e guerra ao dinheiro (proibições e restrições ao uso e posse de dinheiro em espécie, que abundam por todo o mundo).

É crescente o entendimento do “bug do ouro”[262], como detalhado por Micaroni, evidente nas diversas vezes em que o ouro privado foi expropriado, como já aconteceu até nos EUA e hoje ocorre na Índia e na Venezuela[263] – e nas restrições crescentes ao seu uso e transportabilidade.

3.1.1 Bitcoin, Ouro e Fiats no espaço tempo

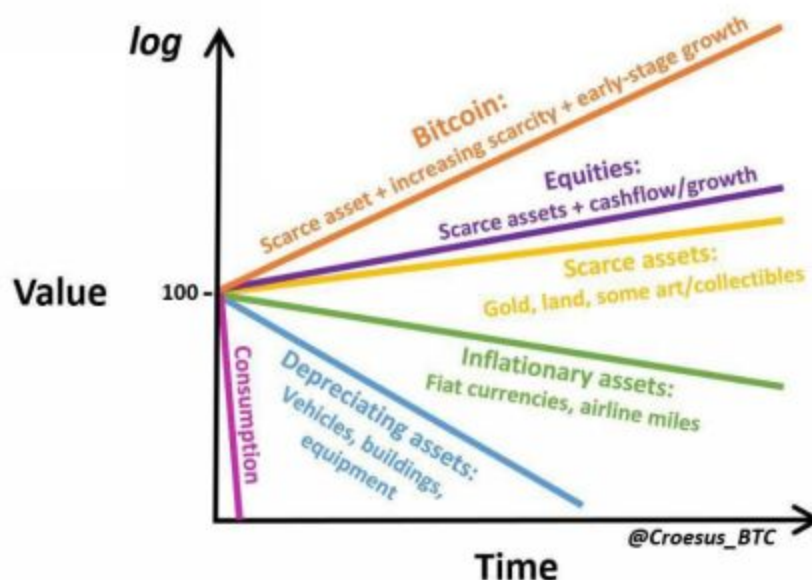
Os Bancos Centrais, quando imprimem mais *fiat*, diluem o valor de todos que possuem a moeda que eles emitem. Sua política econômica expansionista destrói riquezas acumuladas ao longo do tempo. Já na década de 1930, Henry Ford[264] afirmava que se a maioria das pessoas

entendessem como funciona o sistema monetário e bancário: “haveria uma revolução antes do próximo amanhecer”.

Optar pelo Bitcoin é sair do jogo fraudado no qual o honesto não tem como vencer — sem violência. É a alternativa crescente para armazenar, transportar e manter valor no espaço e tempo.

Ouro transporta valor bem no tempo, mas é péssimo no espaço, como ficou claro com quem guardou o metal em Cuba, Vietnã, Venezuela ou outro lugar tomado por ditadura comunista. *Fiats* transportam valor bem no espaço e são péssimas no tempo.

Bitcoin é bom em transportar na escala, no tempo e no espaço. A tendência é que seja, cada vez mais, eficiente em divisibilidade, transportabilidade e durabilidade: mais *halvings e* mais legitimação aumentam sua propriedade de reter valor no tempo (ou até ganhar). Mais soluções (2ª camada, *sidechains*, *offchain*, *etc..)* reduzem os custos de transação, ficando ainda mais transportável, divisível e fungível.

É urgente o amplo acesso a um dinheiro sólido em escala[265] (divisibilidade), espaço e tempo (*sound money)*. Mesmo os bancos já tomaram prejuízos bilionários com falsificação de ouro[266] demonstrando a complexidade para afirmar sua veracidade.

A solução de centralizar a sua custódia nas mãos de governos *(Gold Standard)* e terceiros de confiança foi tentada diversas vezes, mas sem sucesso. Todas as vezes as promessas de conversão, cedo ou tarde, foram desonradas[267].

O Bitcoin pode se provar como uma alternativa viável para o armazenamento de valor, melhorando as deficiências do ouro na propagação no espaço e no tempo. Imune à censura, pode ser enviado para qualquer pessoa no mundo a um custo relativamente baixo ou quase zero pela Internet.

Ouro e Bitcoin podem e devem coexistir. Mesmo que o ouro seja completamente desmonetizado, ele ainda terá valor como insumo industrial.

Alternativas ao ouro físico são *tokens* de *stable* ouro — como PAX Gold (*IOU* de ouro que pode ser enviada pela Internet); e, potencialmente,

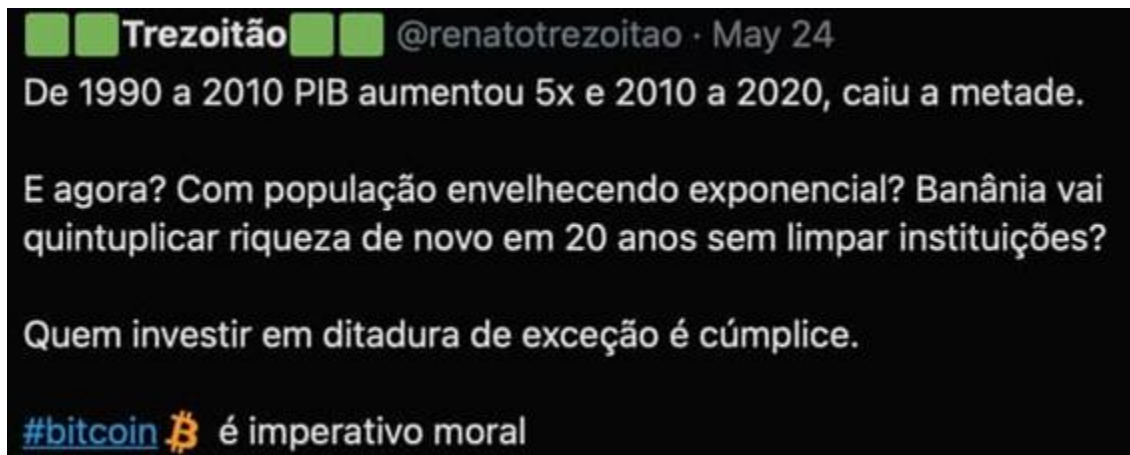
créditos de ouro gerados com colateral de bitcoin (como o *MAKERDAO* gera DAI, *stable* de dólar colateralizado em *crypto*).

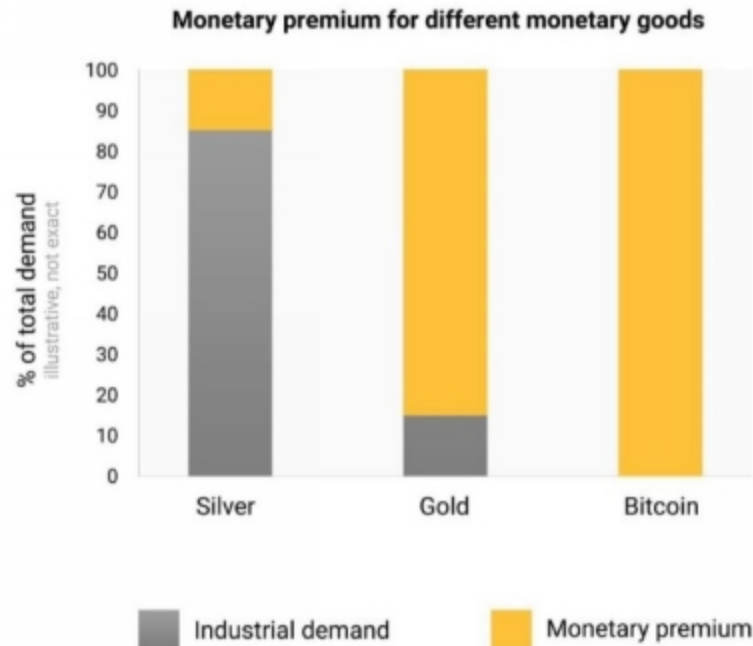
O bitcoin é o colateral supremo, simplesmente porque sua movimentação pode ser verificada publicamente e a sua posse comprovada com baixíssimo custo, por assinatura de chaves.

Se você pega um empréstimo colateralizado da Rispar[268] — ou com sua avó que depende da renda em real, pagando a ela 2 a 3x mais que o CDI (juro real negativo, coitada), quem pega os reais emprestados pode verificar onde os seus bitcoins estão depositados — até mesmo fazendo prova pública de infiel depósito ou estelionato se forem movidos de maneira diversa ao contratado.

Em decorrência disso, grande parte do ouro negociado no futuro, em vez de "ouro de papel" ou "ouro fisico" (com altíssimos riscos de transação, em transporte, certificação e inadimplência) tende a ser "ouro sintético", colateralizado em bitcoin, aumentando ainda mais a demanda por BTC.

A rede *blockchain* do Bitcoin é um sistema de comunicação a prova de censura que possibilita diversas aplicações. Contratos e fatos podem ser registrados na blockchain[269]. A rede, portanto, transporta informações no espaço e tempo de forma segura — e não apenas ativos.

Em poucos anos a riqueza das famílias será mais determinada pelo ano em que começou a acumular BTC do que por sua profissão ou riqueza em outros séculos. Esse será o *RESET* para zerar riquezas obtidas de maneira ilegítima — exatamente devido à tendência sistemática de as elites morais e intelectuais aderirem ao padrão Bitcoin primeiro. Um filtro moral para quem for manter riqueza. Bitcoin é um imperativo moral e pragmático: investir no *legacy* (perda fixa e perda variável) é suicídio financeiro e moral, além de financiamento de crime.

3.1.1.1 Ouro ou Bitcoin? Ou ouro e bitcoin?

O ouro foi a reserva suprema de valor, histórica e global, com um valor total de mercado (*market cap*) de cerca de US$ 12 trilhões[270]. O emprego como reserva multiplica o valor de mercado do ouro muito além do valor derivado da sua utilidade industrial. O metal foi um ativo culturalmente importante por milhares de anos, devido às suas propriedades superiores de dinheiro sobre os demais metais e meios circulantes.

No entanto, o ouro tem algumas desvantagens importantes, nas quais se incluem:

a) **É difícil de transportar e caro armazenar**; exemplo disso é o deságio mais de 50% no preço na Venezuela e em lugares com controles draconianos[271]; e

b) **É difícil verificar qualidade e veracidade[272]**, como resultado, grande parte do ouro do mundo é mantida em repositórios centralizados que seguem diretrizes rígidas[273] – e a maior parte do ouro vendido não tem liquidação física, não servindo de *hedge* nas situações de colapso societal. Um dos problemas do padrão-ouro (*gold standard*) é a impossibilidade de verificar os saldos e a conversibilidade dos depósitos. Essa deficiência é mitigada no Bitcoin, já que os saldos são públicos. Em um depósito consignado de bitcoin, é pública a prova de se os saldos foram ou não movidos e, assim, se estão ou não sob o controle do detentor de certo endereço.

c) **Ouro não é facilmente divisível**. A maior parte do ouro é entesourado na forma de barras, moedas ou joias, o que dificulta a transferência de quantidades exatas. Um grama de ouro, em maio de 2020, custava mais de R$ 300,00. Mesmo nas épocas em que o

ouro era moeda corrente, raras eram as pessoas que teriam a capacidade de fracionar, medir e guardar 30 reais em ouro, daí um dos motivos da monetização da prata e dos trocos de cobre.

O Bitcoin foi criado para emular e melhorar as propriedades que fazem do ouro reserva de valor, como descrito na narrativa de Ouro 2.0, também resolvendo alguns dos inconvenientes do ouro:

a) **Bitcoins são muito fáceis de transportar e armazenar:** Já houve transações nas quais foram transmitidas dezenas de milhares em bitcoins (avaliados em mais de um bilhão de dólares) ao custo de alguns dólares. Esse custo da transação (*fee*) é voluntário, quanto maior o valor pago, maior a chance de a transação ser processada rapidamente, quem tem pressa paga mais, quem não tem paga menos, e, em ambientes *off-chain* e de segunda camada, paga nada ou quase nada por transações imediatas, mas sem os registros públicos perpétuos e o mesmo nível de segurança. Várias corretoras, inclusive brasileiras, permitem trocas de saldos de bitcoin gratuitamente entre a *Lightning Network* e a *main-net*. Armazenar bitcoins é praticamente gratuito, se o titular memorizar as palavras geradoras (*seed phrase*) criadas *off-line* com senha criptografada (*brain wallet* ou *paper wallet* criptografada), então não há como roubar ou *hackear* os bitcoins sem o fornecimento da senha. O custo de usar *softwares* abertos e gratuitos não pode ser comparado com dispendiosos sistemas de cofres e monitoramento. Há dezenas de *wallets* (carteiras) gratuitas para *desktop* ou *smartphone* que acessam rapidamente os saldos quando importadas as palavras geradoras (*seeds*) ou chaves privadas. Por isso, em lugares como a Venezuela[274] , há deságio de ouro e ágio de bitcoin.

b) **Bitcoins são facilmente verificáveis:** Informações sobre cada bitcoin e saldos de cada endereço podem ser vistas na *blockchain* pública do Bitcoin, visível por qualquer pessoa conectada à rede. Os proprietários de bitcoins podem facilmente provar que os controlam (registro de propriedade), inclusive sem movimentar saldos e sem custo, através de assinatura de mensagens com a

chave privada (feita de maneira prática e segura por meio de *hardware wallets* ou gratuita e menos segura por programas gratuitos).

c) **Bitcoin é facilmente divisível**: A menor unidade de um bitcoin – batizada de *satoshi* pela comunidade – é cem milionésimos de um único bitcoin (0,00000001 BTC), portanto é divisível *on-chain* até a oitava casa decimal e é ainda mais divisível *off-chain*, como saldos em corretoras – essas frações de *satoshis* podem ser transacionadas também em segunda camada, como na *Lightning Network*[275].

É crença dos autores que mercados de *tokens* de *stable* ouro (e demais índices e *commodities* significativos), integralmente colateralizados em bitcoin, serão ativos superiores a ouro físico no futuro, tendo mais liquidez, transportabilidade e utilidade para colateral em empréstimos e alavancagem – finalmente resolvendo os problemas do padrão-ouro.

Os *tokens* atualmente oferecidos de *stables* (dólar, ouro ou qualquer outro bem), se não forem integralmente colateralizados em cripto (como *DAI* do *maker DAO*), apresentarão riscos de custódia compostos (do emissor, da *blockchain* em que estão registrados e de onde estiverem depositados) e estímulos ao oportunismo os inviabilizarão no longo prazo.

Classificação das principais características dos ativos: Bitcoin, Ouro e Moeda fiduciária[276]:

	Bitcoin	Gold	Fiat
Durable	B	A+	C
Portable	A+	D	B
Fungible	B	A	B
Verifiable	A+	B	B
Divisible	A+	C	B
Scarce	A+	A	F
Established History	D	A+	C
Censorship Resistant	A	C	D

O Bitcoin é um candidato emergente a ouro digital. Levará tempo e um histórico de desempenho em vários ciclos de mercado para que o Bitcoin seja amplamente considerado como uma reserva de ativos de valor equivalente ao ouro físico.

Como é natural na evolução de ativos monetários em suas funções (meio de troca, reserva de valor, unidade de conta...), as narrativas sobre o bitcoin têm evoluído: na primeira, o sistema era visto como meio de pagamentos barato e rápido, para substituir as moedas fiduciárias.

Na segunda Era, com aumento das *fees* e da cotação, a narrativa dominante passou a ser a de moeda para usos mais nobres, como remessas imunes a controles de capitais ou pagamentos com certo nível de privacidade (para mercados como *silk road*).

No terceiro ciclo, dominava a narrativa de ouro digital, com as identificações de padrões de valorização exponencial (como o *bitcoin rainbow chart* e o *S2F*[277]).

Na quarta Era, o bitcoin é considerado como ativo financeiro essencial para diversificação e aumento de potência de carteiras, dados seus índices de risco/retorno[278] e correlações; assim como, com a legitimação do BTC (demonstrada pelo desenvolvimento de mercados futuros, participação institucional e regulação crescente).

Diversos bilionários (como Peter Thiel, Jack Dorsey, Chamath Palihapitiya, Tim Draper, Mike Novogratz, Michael Saylor e outros) e personagens respeitados em mercados convencionais (como Ray Dalio[279] e Paul Tudor Jones[280]) recomendaram e admitiram ter adquirido bitcoins como meio de elevar rentabilidade por diversificação.

TEXAN HODL @TexanHodl · 4h

Ray Dalio 1 month ago: The US Government will ban bitcoin.

Ray Dalio today: I'd rather own bitcoin than a bond.

The tides are turning 👀

4. (How, How Much?) Como e quanto?

O Bitcoin resolveu de forma não violenta o consenso do “Problema dos Generais Bizantinos”[281], conhecido como “Falha Bizantina”[282], na área da computação, por meio da mineração por prova de trabalho (*Proof of Work - PoW)*[283].

O sistema resolve a questão de qual bloco reconhecer se dois mineradores emitirem simultaneamente informações diferentes, reconhecendo como válida a cadeia que apresentar maior prova de trabalho. É isso que o consenso de Nakamoto utiliza para resolver o problema dos gastos duplos: maior prova de trabalho. Por isso, quanto maior *hashrate*, mais caro é um ataque viável à rede, em termos de energia elétrica a ser empenhada executá-lo.

A partir de 2020, o bitcoin se tornou a forma de dinheiro mais escassa já inventada, momento em que sua inflação passou a ser menor que a do ouro (percentualmente, os novos bitcoins adicionados ao estoque já existente representam menos do que o novo ouro minerado em relação a todo o ouro que existe). Sua valorização contribui ainda mais para tornar a sua rede mais segura e imune a ataques.

Mais indicações do porquê o Bitcoin manter uma dominância altíssima dentre as criptos são: maiores Efeito Lindy[284] e Efeito Rede[285]; maior respeito à Lei de Gall[286] (mantendo complexidades e vulnerabilidades consequentes fora da camada base); e, por que, nas análises fundamentalistas de cripto, o *hashrate* é usualmente indicado como elemento inicial. O bloco com menor prova de trabalho e as transações nele contidas serão posteriormente reprocessados (se já não estiverem na *blockchain*).

O Bitcoin, como rede descentralizada, remunera os mineradores (com os valores das *fees* e dos novos bitcoins) pela capacidade computacional despendida (medida pela prova de trabalho).

Ele funciona com geração de estímulos de mercado que regulam a atuação dos mineradores (investindo mais ou menos em energia elétrica e equipamentos a depender dos seus custos de operação e da cotação do bitcoin, gerando um mercado mundial de energia elétrica, mesmo que produzida longe dos polos de consumo tradicionais); e dos usuários (investindo mais ou menos em *fees* e buscando mais ou menos soluções

alternativas de pagamentos, como a *Lightning Network*, *Liquid* e transações *off-chain*).

4.1 Bitcoin e o gasto de energia

Há amplas alegações[287] de que a mineração por *PoW (proof of work)* é um desperdício e prejudicial ao meio ambiente. Essa argumentação é puramente mentirosa[288]. A maior parte da energia utilizada na mineração é renovável e limpa (em muitos casos é energia ociosa, que seria desperdiçada), subsidiando a produção e distribuição de mais energia, com economias de escala e escopo.

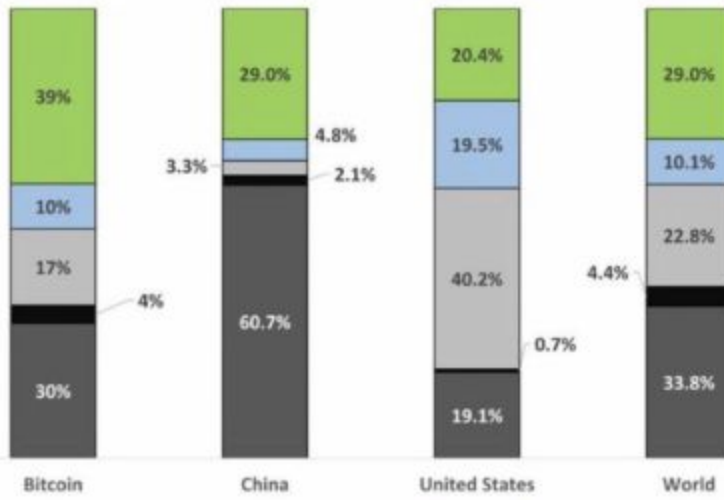
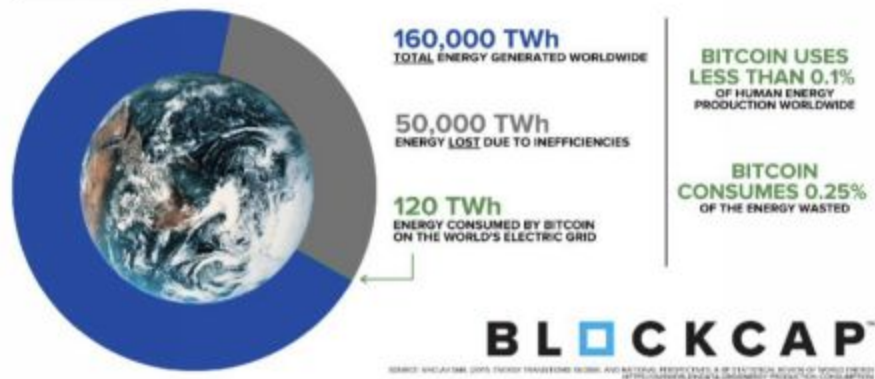
Mineração garante valor piso de energia, viabilizando projetos (inclusíve os de energia renovável) uma vez que estabiliza demandas intermitentes e reduz risco de não haver demanda local suficiente – além de previnir custos (institucionais, energéticos e ambientais) da mineração de ouro, da impressão de notas e manutenção de instituições bancárias.

Mesmo que essas refutações não fossem verdade, quem define o melhor uso de qualquer bem é seu dono. Se há pessoas dispostas a empregar seus recursos em bitcoins[289] e há pessoas dispostas a empregar seus recursos em máquinas e instalações para minerar bitcoins, está provado que o sistema é otimizado pelos mecanismos de mercado.

De fato, o Bitcoin hoje já consome mais energia[290] que países com milhões de habitantes, só que a questão ambiental deve ser considerada em termos de custos de oportunidade: qual o custo ambiental da produção do ouro (majoritariamente usado para reserva de valor), além do custo energético com a destruição do solo e contaminação química de cursos d'água? Para onde iria a energia ociosa? O custo mundial da energia cairia ou subiria se não houvesse o mercado de mineração de bitcoin garantindo um nível mínimo de remuneração pela energia, sem demandar qualquer infraestrutura de transmissão até centros urbanos ou industriais?

Carros consomem mais energia que carroças – que consomem mais que caminhar. Computadores consomem mais energia que máquinas de escrever – que consomem mais que caligrafia à mão. A evolução tecnológica normal é de mais consumo de energia em soluções superiores. Quem for realmente sincero em sua intenção de reduzir consumo de energia deve parar de usar computadores, máquinas de lavar, geladeiras e utensílios domésticos elétricos em sua casa, para começar.

Segundo diversas fontes[291] o Bitcoin é a indústria mais limpa do planeta e consome menos de 0,25% da energia ociosa (desperdiçada):

Electricity Mix (2020) - Bitcoin vs. China vs. USA vs. The World
39%
10%
17%
4%
30%
29.0%
4.8%
3.3%
2.1%
60.7%
20.4%
19.5%
40.2%
0.7%
19.1%
29.0%
10.1%
22.8%
4.4%
33.8%
Bitcoin
China
United States
World
Sources:
CBECI.org
ourworldindata.org/electricity-mix
Coal
Oil
Gas
Nuclear
Renewables (Incl. Hydro)
Hass McCook, May 2021, @FriarHass

Estimativas[292] indicam que as transações na *Lightning Network* são 3,7 milhões de vezes mais eficientes (em consumo de energia) que uma transação usando cartão de crédito. A economia *onchain* medida em W/GH (*Watts por Gigahash*) aumenta sistematicamente:

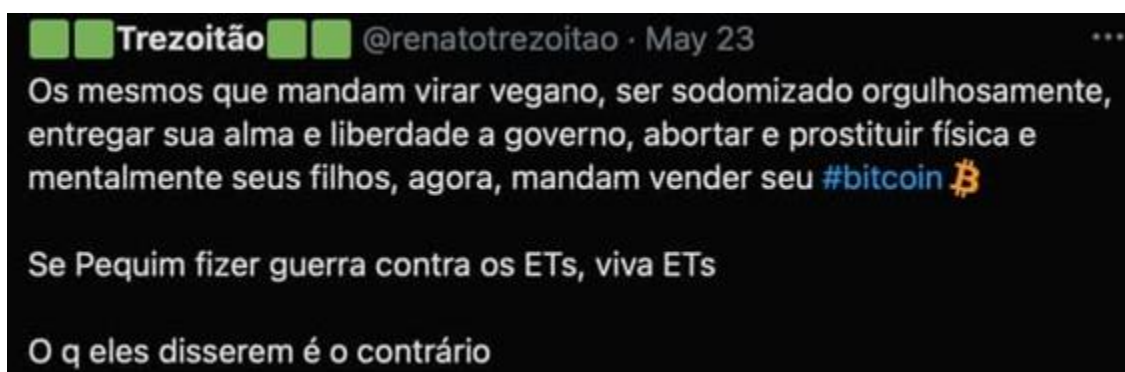
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Hash Rate (Gh/s)	0.003	0.575	0.550	0.650	63	878	4,255	9,750	11,500	22,550
Watts	55	241	271	250	445	509	1,145	1,200	1,450	1,786
Price (Release)	104	540	369	550	1,299	460	1,553	1,494	1,100	1,709
Efficiency (Gh/W)	**0.00005**	**0.002**	**0.002**	**0.003**	**0.16**	**1.7**	**3.7**	**7.9**	**7.9**	**12.4**
y/y		*4749%*	*-14%*	*27%*	*6190%*	*923%*	*121%*	*112%*	*1%*	*56%*
Hash Rate Cost ($/Gh)	**$39,808**	**$938**	**$671**	**$846**	**$21**	**$0.5**	**$0.4**	**$0.2**	**$0.1**	**$0.1**
y/y		*-98%*	*-28%*	*26%*	*-98%*	*-97%*	*-30%*	*-58%*	*-38%*	*-21%*

A classificação *ESG*[293]*(Environmental, Social and Governance)* é amplamente considerada forma de subversão[294] e sabotagem das economias do ocidente, vez que empobrece famílias e países.

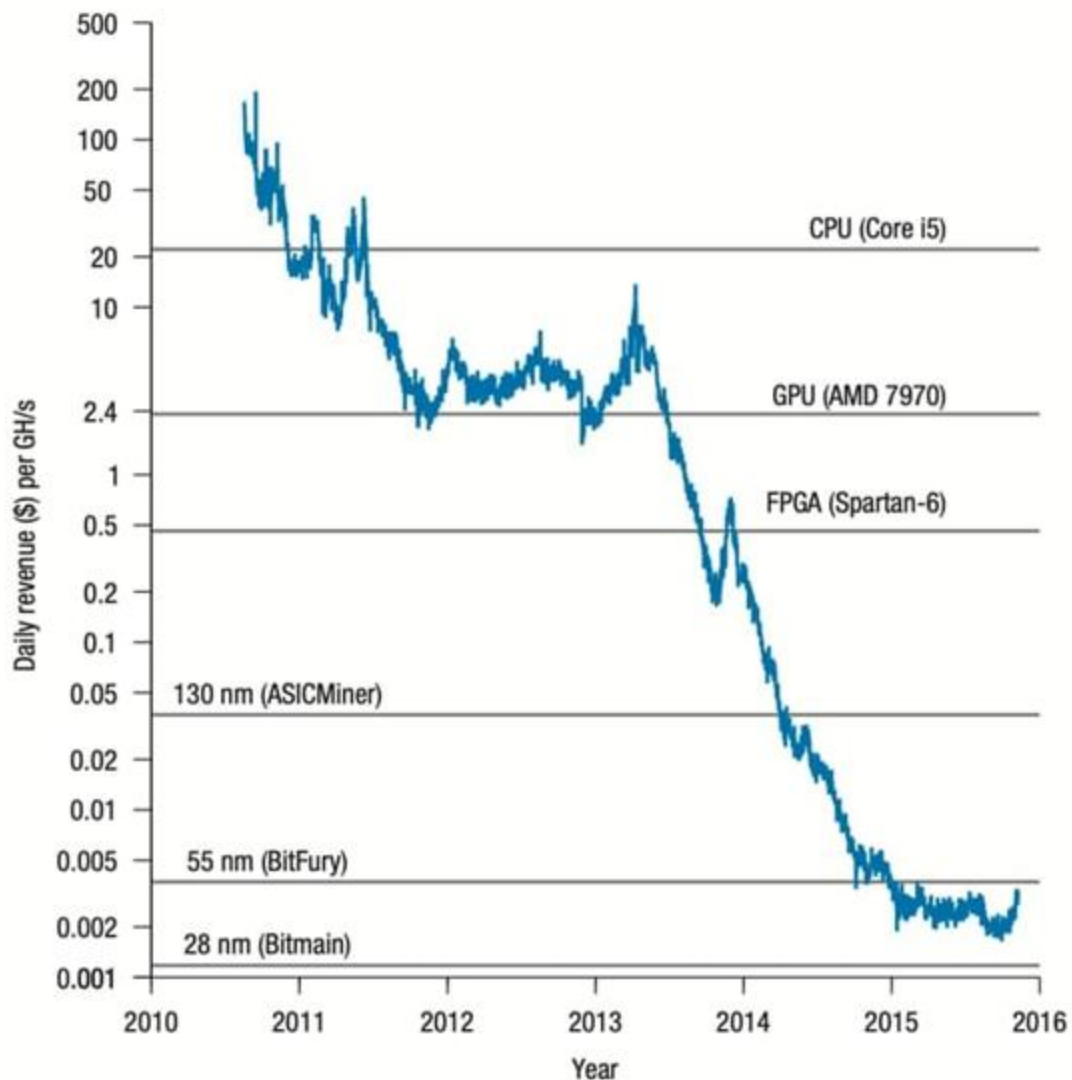
Com base nos dados sobre a mineração do Bitcoin, pode-se concluir que não há outra alternativa: a) mais benéfica ao meio ambiente (viabilizando economia de escala a projetos de produção de energia, ao resolver problema da energia ociosa e reduzindo uso de alternativas mais poluentes); c) mais benéfica à sociedade, porque resolve conflitos sem violência e gera riqueza e com a restauração de direitos individuais de livre expressão, de transação,

de propriedade e de acesso a dinheiro forte; e d) com governança superior (consenso não violento, com incentivos à cooperação).

Assim, qualquer alegação em contrário é um ataque de contrainteligência, com intuito de subverter sociedades, corporações, famílias e indivíduos – usando propaganda para fazê-los renunciar a tecnologia que os faria mais ricos e livres.

Exemplos de atos de guerra baseados em infiltração, subversão e contrainteligência – convencendo pessoas e instituições a ter comportamentos contrários aos seus próprios interesses e intenções são: o *financial welfare* da China[295] e "Coreia da Morte[296] contra os Estados Unidos — atraindo empresas com a promessa de acesso ao seus mercados gigantescos e baixo custos de operação a fabricar seus seus bens lá (para receber roubo massivo de propriedade industrial, expropriações e chantagens), o uso da Peste de Wuhan como arma biológica e de engenharia social[297]; ou mesmo financiamento público a militância anti patriótica racialista (como o projeto 1619 e o BLM) ou ao marxismo cultural dominante na academia ocidental[298].

Não faz diferença se a COVID foi fabricada e espalhada dolosamente, vazada culposamente ou foi criada e dispersada legalmente: se a ditadura comunista escondeu ilegalmente sua existência[299] (prendendo e torturando médicos que diziam a verdade, como Li Wenliang) e mentiu afirmando que se tratava de zoonose não transmissível entre humanos, inclusive usando OMS[300] aparelhada de militantes comunistas corruptos para confirmar narrativa, cada centavo gasto ou destruído com a fraudemia é responsabilidade dessa ditadura criminosa.

Outros exemplos atuais de ataques de engenharia social para convencer governos e populações a renunciarem a liberdade e riqueza são: a) *lobby* para países renunciarem a energia atômica; b) militância contra o consumo e produção de carne e proteína animal[301] (apenas veja o físico de Bill Gates[302]: com suas mamas, culotes e pança para concluir se ele pode te dar recomendações de saúde e alimentação); c) obrigatoriedade de focinheiras[303] de pano insalubres que aumentam transmissão de doenças por fômites; e, d) políticas de confinamento de saudáveis inocentes (*lockdown*) denunciada[304] por milhares de cientistas como totalmente prejudicial e sem qualquer evidência científica, empírica ou lógica, que a fundamente (além da intenção política de aumentar poderes e rendas dos donos do governo).

Retomando a questão da mineração, a evolução da eficiência dos *hardwares* que usam chips *ASIC (Application-Specific Integrated Circuit)* adaptados para minerar Bitcoin, com base em um algoritmo de *hash* específico, está diminuindo (assim como na indústria de *hardware* em geral, a Lei de Moore não é mais constante). À medida que a vantagem competitiva de estar no estado da arte diminui, podemos esperar um aumento na concorrência dos fabricantes, à medida que as margens diminuem, como podemos ver na imagem[305]:

Quando a energia usada para *PoW* * irá * parar de crescer? Precisamente quando produtores de energia suficientes começarem a fazer *PoW* diretamente, o retorno marginal da queima de kWh de energia através de *PoW* = o retorno marginal da venda desses kWh à rede – quando o “prêmio” no *PoW* é

reduzido a zero. Eu chamo esse equilíbrio de "ponto de Nakamoto". Suspeito que o *PoW* usará entre 1 e 10% da energia do mundo quando esse equilíbrio for alcançado.

Dhruv Bansal[306]

Alguns reclamam que a mineração de Bitcoin não realiza "nada de útil", como encontrar números primos. Embora a introdução de uma recompensa secundária por fazer o trabalho possa parecer uma ideia virtuosa, na verdade, introduz um risco de segurança. Dividir a recompensa pode levar a uma situação em que "vale mais a pena fazer a função secundária do que fazer a função primária". Mesmo se a função secundária fosse inócua (um aquecedor), em vez de US $ 100 por x *hashes*, nós passaríamos para US $ 100 + US $ 5 de calor por x *hashes*. O "Aquecedor de Mineração" é apenas mais um aumento na eficiência do hardware, resultando em uma maior dificuldade e um aumento em (energia utilizada / bloco). Felizmente, o Bitcoin nunca terá esse problema, pois sua segurança é garantida pela pureza de seu algoritmo de prova de trabalho.

Noah Ruderman

4.1.1 Bitcoin, otimização de energia e desinformação

Além de Elon Musk, outros magnatas do setor de energia estão investindo e estudando o potencial do Bitcoin, como alternativa de reserva de valor e meio de demanda constante, garantindo valor “piso" da energia gerada, mesmo a ociosa, que seria perdida de outra maneira.

Exemplos são Carl Icahn e Røkke, CEO da *Aker*[307]. A *Aker* criou uma subsidiária, *Seetee*, dedicada ao investimento em Bitcoin e projetos relacionados ao ecossistema. A nova unidade promete uma estratégia tripla: investir em bitcoin como seu ativo de tesouraria, investir em projetos e empresas cripto e implementar operações para a mineração de bitcoin.

Em carta[308] aberta aos *stakeholders* da *Seetee*, Røkke comenta como o bitcoin pode ser a forma de "bateria" definitiva para viabilizar energias alternativas intermitentes (como solar e eólica). Quando os componentes do

hardware de mineração virarem *commodity*, qualquer energia ociosa, em qualquer lugar do mundo, poderá ser convertida em bitcoin.

Nessa carta, o presidente da Aker fez afirmações interessantes:

> A criação da *Seetee* é resultado de uma discussão longa e fundamental sobre valor e acredito que o Bitcoin é superior ao dinheiro físico e ainda melhor do que o ouro. […] Estamos acostumados a achar que o dinheiro físico é livre de riscos. Mas não é. É explicitamente taxado pela inflação com uma pequena taxa a cada ano. […] O bitcoin é como o ouro, mas bem melhor. […] As pessoas que mais sabem sobre Bitcoin acreditam que seu sucesso futuro seja quase inevitável, enquanto o outro lado acha que seu fracasso é quase certo. A situação atual não é possível. [livre tradução]

Um *whitepaper*[309] lançado pela *Square* (empresa de pagamentos de Jack Dorsey) com a participação da *Ark Invest*, intitulado “Bitcoin é a chave para um futuro de energia limpa e abundante”, propõem que o Bitcoin é o caminho para um futuro sustentável. O *paper* foi lançado como parte da *Bitcoin Clean Energy Initiative*[310].

Há também estudos interessantes sobre consumo de energia do Bitcoin, feito por empresas importantes do setor como a *Coinshares*[311] e *Galaxy Digital*[312].

Como resta evidente, o Bitcoin funciona majoritariamente com energia ociosa e pode até ser considerado uma “bateria global”. Mesmo quando não é utilizada energia energia ociosa, não há retirada de energia usada em qualquer uso mais nobre, considerando que as margens de mineração são baixíssimas.

A mineração de Bitcoin aproveita energia desperdiçada, mitiga a destruição de capital e fornece um mecanismo para comercializar energia limpa e renovável onde quer que a encontremos. Com a tecnologia atual, as energias renováveis não podem substituir os combustíveis fósseis (hidrocarbonetos) por completo sem impactar brutalmente no padrão de vida da humanidade – como ficou evidente na crise energética do Texas em 2021[313].

Painéis solares, pás (ou hélices) de usinas eólicas e baterias também apresentam impactos ambientais brutais[314], usualmente ignorados no debate público – devido aos custos de sua fabricação e de descarte.

A febre dos carros elétricos – sejam alimentados por baterias ou por células de hidrogênio – também é uma distorção resultante dos juros negativos e de captura administrativa, corrompendo políticas públicas. Esses veículos nunca foram viáveis sem quantidades brutais de subsídios – e talvez não sejam em décadas.

Defender um sistema baseado puramente em energias renováveis[315] significa defender energia mais cara e menos oferta de energia, tornando a sociedade mais dependente e pobre. Em regra, uma rede totalmente dependente de energias renováveis coloca a sociedade à mercê do clima favorável ou de importação de energia – como ficou claro na Alemanha, com energia caríssima e prostrada em submissão aos vizinhos, dos quais depende de importação[316].

O Bitcoin contribui para que novos projetos sejam desenvolvidos e viabilizados garantindo demanda fixa com preço mínimo. Toda infraestrutura de mineração de bitcoin também pode se beneficiar da energia nuclear, tida também como não poluente[317] em que os rejeitos são, cada vez mais, recicláveis[318]. Até mesmo bilionários globalistas como Bill Gates, investem pesadamente em projetos de energia nuclear[319].

Existe ainda uma batalha árdua sobre o combate à desinformação sobre a mineração de bitcoin, por isso muitos na comunidade produzem diversos artigos, vídeos e livros para desmistificar a mentira de que "o bitcoin é deletério para o meio ambiente”.

Outro movimento de desinformação é o *"The Great Reset"[320]* promovido por organizações globalistas[321] com o objetivo declarado de promover reengenharia social e econômica mundiais. Segundo eles, a “única saída" para crise do Covid-19 (“pandemia”) é um “mundo melhor” no “novo normal”, como a redefinição do contrato social (o Estado interferindo ainda mais na vida das pessoas, ou seja, socialismo implementado por meio de mais controle) e a agenda ESG *(Environmental, social and corporate governance*)[322] juntamente com a agenda ambientalista alarmista (como a descarbonização).

Um dos objetivos do "Grande *Reset”*[323]: "Você não terá nada e será feliz.”. Se discordar e quiser ter patrimônio, liberdade e honra, basta desinvestir do *legacy* e comprar bitcoin.

Bilionários (cantillonarios), celebridades (progressistas) e as elites[324] mundiais não querem que você possua nada e afirmam que você será feliz. Benjamin Franklin já dizia que: "Aqueles que abrem mão da liberdade essencial por um pouco de segurança temporária não merecem nem liberdade nem segurança."

4.2 Mineração, endereços e ajustes

O mecanismo de ajuste de dificuldade (entre *hashpower* e tempo médio de criação de blocos) da rede Bitcoin fornece correção necessária para os mineradores a cada 2016 blocos.

Se o *hashpower* (poder computacional) subir de maneira significativa até o ajuste, os blocos tenderão a ser produzidos em média mais rapidamente, aumentando a emissão diária de bitcoins – por isso, não há previsão exata dos futuros *halvenings* (porque dependem do número de blocos minerados e o tempo para que isso ocorra pode ser reduzido se houver aumentos repentinos de investimentos em mineração).

Os blocos são gerados a cada 10 minutos, em média. Tende a ser mais rápido quando o *hashrate* aumenta e, em sentido contrário, tende a demorar mais quando o *hashpower* total aportado na rede cai.

O ajuste de dificuldade é a tecnologia mais confiável que existe para produzir uma moeda forte e controlar a taxa de escassez. Sem esse mecanismo e com o poder de mineração aumentando exponencialmente, todos os bitcoins já teriam sido minerados.

Outro mito repetido por quem não compreende os mecanismos de ajuste entre mineração e preços de mercado é o “preço mínimo de mineração viável”, abaixo do qual haveria uma “espiral da morte”. Ora, se há mais empresas minerando, então os bitcoins emitidos vão ser divididos entre mais agentes.

Se a cotação do bitcoin cair brutalmente e metade dos mineradores deixarem de operar (devido a seu custo de operação ficar acima do valor dos bitcoins recebidos), as *fees* e os novos bitcoins (subsídio) serão divididos pela metade entre os mineradores que continuarem (aumentando sua remuneração até haver equilíbrio de mercado).

Então, se o bitcoin cair de 50 mil para mil dólares, a “morte” poderá acontecer para os mineradores com maiores custos de operação, mas, para os operadores de menor custo, a operação continuará viável, pois receberão mais bitcoins com menor valor unitário. O sistema se autorregula até o

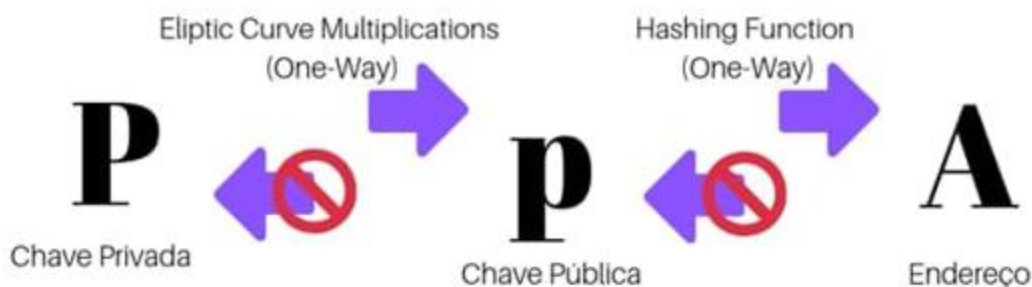
equilíbrio, a mineração continua sendo viável em algum nível com qualquer preço atual ou futuro positivo de bitcoin.

Se for considerado o fato de que agentes mineram para adquirir fluxo de caixa em bitcoin sem considerar custo de operação imediato – por exemplo, por *hobby* ou por já ter vendido os bitcoins em mercado futuro ou feito *hedge* com opções –, então, não existiria “preço mínimo de mineração”, pois esses mineradores continuariam a operar independentemente da cotação corrente.

O Bitcoin permite a criação de chaves (públicas e privadas) e endereços *off-line* (sem acesso à Internet*).* Os endereços[325] são sequências alfanuméricas derivadas de chaves públicas para o recebimento de bitcoins.

Para movimentar os saldos ou comprovar sua propriedade com assinatura de mensagens, é necessário acessar as suas chaves privadas.

Os endereços são equivalentes às contas bancárias e as chaves privadas equivalentes às senhas para sacar ou transferir seus saldos.

Uma analogia didática ao funcionamento é o *e-mail*: quem souber seu endereço de *e-mail* pode enviar mensagens para esse endereço; e quem tiver a senha (chave privada) desse *e-mail* pode mandar mensagens a partir dele. A particularidade é que *e-mails* não podem ser criados *off-line*, como endereços de bitcoin[326]:

O bitcoin é divisível por possuir seu próprio sistema de unidade de medida, dotado de até oito casas decimais, a última delas sendo nomeada

satoshi (centésimo milionésimo de bitcoin). Considerando uma cotação de 100.000 USD por bitcoin, um *satoshi* valeria 0,001 dólar, extremamente divisível.

Créditos de bitcoin, negociados em segunda camada ou *off-chain*, como na *Ligthning Network, t*ambém permitem transações de frações de *satoshis*, sendo ainda mais divisíveis nesses ambientes.

Há diversas propostas para aumento das casas decimais no futuro, quando o bitcoin valer milhões ou bilhões de dólares, demandando apenas alteração no protocolo através de *soft fork* ou *hard fork* a depender das questões técnicas, isso é proposto através de um BIP *(Bitcoin Improvement Proposal)* [327].

As moedas tradicionais (dólar, real ou euro) costumam ser divididas apenas até sua centésima parte, o chamado centavo ou cêntimo. No caso do real, 1 centavo = R$ 0,01. Cada bitcoin tem apenas existência digital na rede de computadores que constitui o sistema Bitcoin, muitas das vezes representado por unidades como 1 mBTC, 1 *satoshi* ou 1 µBTC; mas a unidade que possui mais uso no sistema é o *satoshi*, homenagem a Satoshi Nakamoto, criador do sistema Bitcoin.

Na figura abaixo[328], apresentam-se as siglas, os nomes e unidades de medida do bitcoin:

Satoshi	=	฿	
1 Satoshi	=	0.00000001 ฿	
10 Satoshi	=	0.00000010 ฿	
100 Satoshi	=	0.00000100 ฿	= 1 Bit / µBTC (you-bit)
1,000 Satoshi	=	0.00001000 ฿	
10,000 Satoshi	=	0.00010000 ฿	
100,000 Satoshi	=	0.00100000 ฿	= 1 mBTC (em-bit)
1,000,000 Satoshi	=	0.01000000 ฿	= 1 cBTC (bitcent)
10,000,000 Satoshi	=	0.10000000 ฿	
100,000,000 Satoshi	=	1.00000000 ฿	

O bitcoin é progressivamente (assintoticamente) mais escasso (emissão decrescente), pois sua política monetária é previsível, ao contrário do sistema monetário convencional, no qual os Bancos Centrais podem imprimir o quanto quiserem determinados por decisões políticas.

Nunca haverá mais de 21 milhões de bitcoins. Em abril de 2019, havia em circulação em torno de 18,3 milhões[329]. O último subsídio (novos

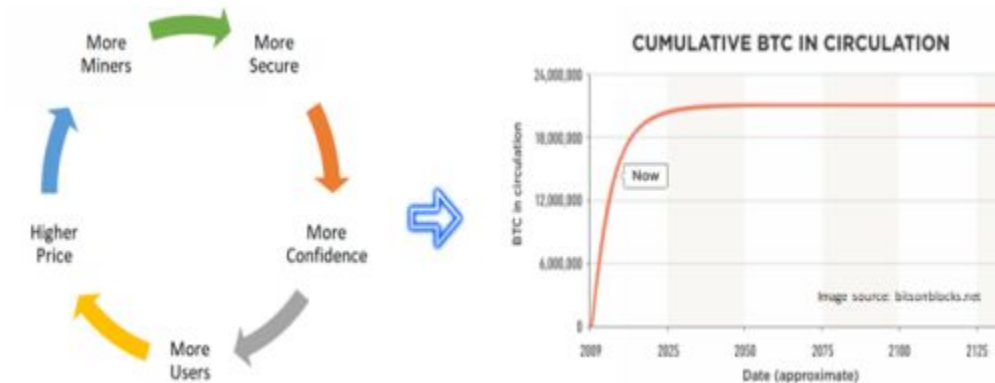
satoshis criados para remunerar mineradores) está previsto para ser minerado no ano de 2140 (quando se espera que o sistema continue funcionando apenas remunerado pelas *fees*, ou sejam introduzidas mais casas decimais para a emissão de subsídios). Sua emissão é controlada pelo algoritmo de código aberto desinflacionário que já existia desde sua proposta original.

Como Nick Szabo[330] denominou, um bem monetário deve ter “custo imprevisível”. Em outras palavras, o bem não deve ser abundante ou fácil de obter ou produzir em quantidade. A escassez é provavelmente o atributo mais importante de comparação entre reservas de valor (como no modelo do *S2FX – stock to flow cross-asset model*), pois, como demonstrado por *PlanB* (investidor institucional holandês), há correlação direta entre medidas de escassez (*S2F*) e *market cap total.*

Outro importante ensinamento do "mestre silencioso" Nick Szabo é que o segredo do sucesso do Bitcoin não está necessariamente relacionado a seu consumo prolífico de recursos ou à escalabilidade computacional, mas requer algo ainda mais valioso: a escalabilidade social *(social scalabity)* em seu *design*, através da segurança.

Escalabilidade social é a habilidade que uma instituição tem de alcançar um número maior de participantes em um esforço comum. Exemplos de instituições socialmente escaláveis (que reduzem custos de transação e conflitos entre usuários) são linguagem, lei e religião.

A figura abaixo[331] demonstra um modelo do círculo virtuoso mencionado em função de sua base monetária com inflação decrescente: o valor do Bitcoin seria atribuído a sua segurança (em vários níveis) derivada da sua descentralização e resistência à censura; que, por sua vez, reforçam a credibilidade da escassez, que é a base do armazenamento de propriedade de valor do bitcoin.

Descentralização e o cronograma de emissão

Por exemplo, deve ser muito difícil para qualquer participante ou intermediário criar dinheiro (para diluir a curva de oferta, levando a uma inflação indevida ou inesperada).

> Em resumo, todo o dinheiro que a humanidade já usou foi inseguro de uma maneira ou de outra. Essa insegurança se manifestou de várias maneiras, da falsificação ao roubo, mas a mais danosa dentre todas provavelmente foi a inflação.
>
> Nick Szabo

O bitcoin é, em diversos aspectos, o ativo mais transportável já criado e o primeiro dinheiro que pode ser transmitido por qualquer meio de comunicação. Para transacionar *onchain,* é necessária alguma conexão com a *internet*, mas transações *offchain* também são possíveis, por exemplo, com dispositivos como *Opendime*[332] da *Coinkite.*

Muitas vezes, ouro físico em território controlado por Estados falidos (como Coreia do Norte, Venezuela ou Cuba) não vale nem metade do que em mercados livres.

Onde há controle de capitais draconianos, não é viável sair legalmente com posse de ouro. A senha para acesso a seus bitcoins pode ser memorizada, enviada por carta, rádio, *e-mail* ou inserida em *hardwares* criptografados (ou até expressa em furos em um cartão como no caso da

Stackbit[333]). A única maneira de impedir o transporte de bitcoins é impedir toda a forma de comunicação.

O bitcoin é difícil de falsificar: por usar a rede *blockchain* para registro perpétuo de transações, o sistema se mostra inviável de ser adulterado permanentemente; até o momento o único problema[334] crítico que foi explorado ainda no início da rede (2010) foi o *bug*[335] que inflou[336] a oferta de bitcoins e que logo foi resolvido via *fork* juntamente com uma atualização de *patch* (correção de código)[337]; após terem resolvido toda a situação, os desenvolvedores entraram em contato com todos os mineradores da época e solicitaram que todos atualizassem as suas versões do *software* e retornassem as transações anômalas.

Maximalistas consideram *altcoins* como falsificações do bitcoin.

Não é possível criar um bitcoin falso sob quaisquer condições. O ataque conhecido como ataque de 51%[338], quando um atacante consegue obter mais de 51% do poder computacional da rede, só consegue desfazer transações, refazendo blocos já minerados.

Trata-se de ativo escasso que é armazenado em uma carteira digital, registrado na *blockchain* de forma publicamente auditável (análoga a um registro de propriedade), podendo ser acessado de qualquer lugar via uma conexão de Internet (ou *off-line* via novas tecnologias sendo aprimoradas, como a de acesso via satélite ou ondas de rádio).

Especialmente após os escândalos dos *Paradise Papers* e *Panama Papers*, das regulações como a *FATCA* e as padronizações de *compliance* como *KYC/AML* (*know your customer* e *anti-money laundering*), os paraísos fiscais e regulatórios para *offshores* se tornaram, mais e mais, inseguros e suspeitos: basta os dados vazarem ou a política oficial do país mudar que se pode perder tudo e todas as transações se tornarem públicas.

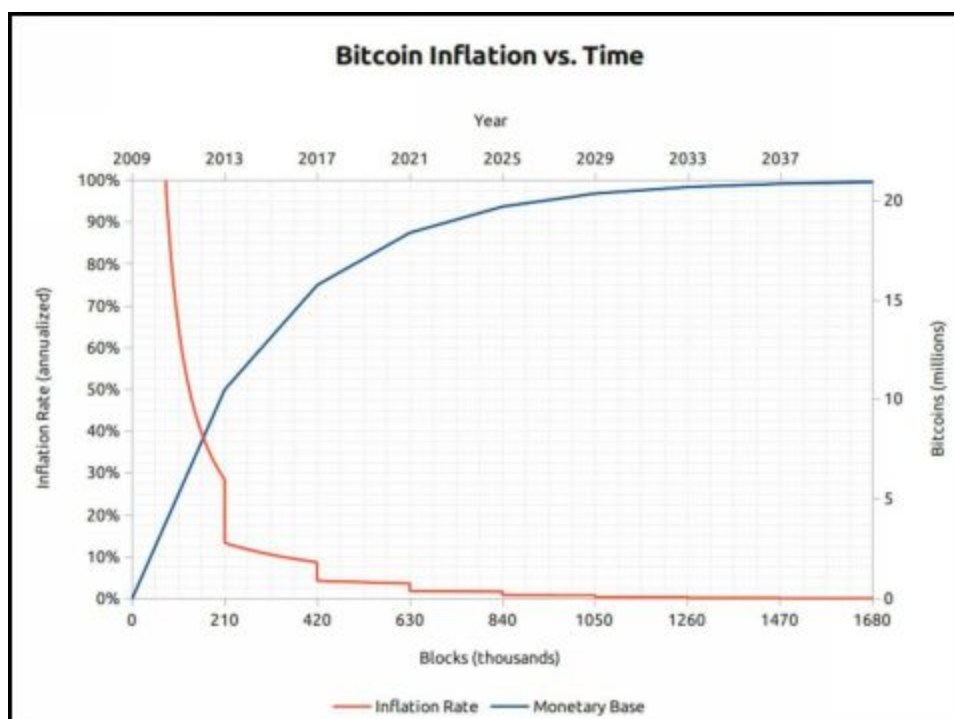
Saldos de criptomoedas podem ser memorizados, por exemplo, através das sementes (*seeds*) geradoras das chaves (12, 18 ou 24 palavras). Essas matrizes (ou as transações derivadas delas) podem ser enviadas por rádio, telefone, *e-mail* ou anotadas em qualquer pedaço de papel e que podem, por sua vez, ser criptografadas para que alguém que capture a mensagem não possa acessar o saldo. Por isso as *hardware wallets* mais seguras são *air gapped* (nunca acessam Internet e são fisicamente isolados). A transação pode ser feita com retirada com cartão de memória, como na *Coldcard* da *Coinkite* (ou pode ser feito até em *tablet* ou celular velho, baixando *wallet* q rode *offline*, como *Samourai*).

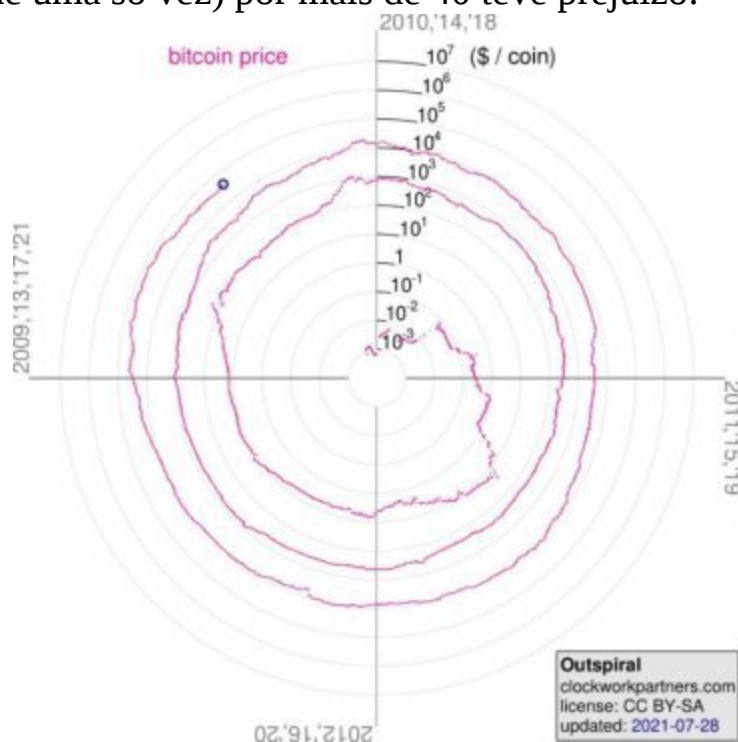
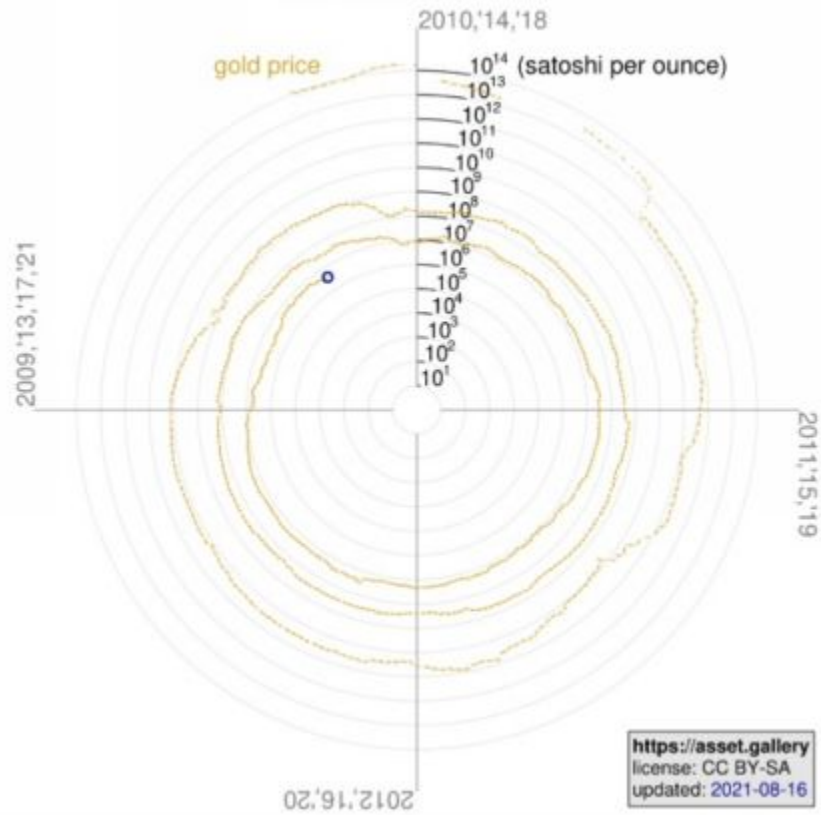
4.3. Halving do Bitcoin: política monetária

A política monetária do Bitcoin possui uma emissão desinflacionária predeterminada. Ou seja, a inflação é decrescente em ritmo logarítmico com emissão caindo à metade a cada 210.000 blocos ou 4 anos, aproximadamente, em um processo chamado *halving*[339]. Predeterminação de emissão e desinflação são os opostos das políticas monetárias da maioria dos governos.

Processo do Bitcoin *halving*, que irá torná-lo menos inflacionário até chegar próximo a sua oferta limite de 21 milhões (assintoticamente):

Evento	Data	Sequencial do bloco	Recompensa do bloco	Total de novos bitcoins entre os eventos
Lançamento do Bitcoin	3 de janeiro de 2009	0 (bloco Gênese)	50	10.500.000
Primeiro halving	28 de novembro de 2012	210.000	25	5.250.000
Segundo halving	9 de julho de 2016	420.000	12,5	2.625.000
Terceiro halving	11 de maio de 2020	630.000	6,25	1.312.500
Quarto halving	**Esperado para maio de 2024**	**840.000**	**3,125**	**656.250**
Quinto halving	Esperado para 2028	1.050.000	1,5625	328.125

A cada quatro anos, o número de bitcoins produzidos como subsídio aos mineradores é reduzido à metade. A emissão de novos bitcoins inteiros deve terminar, aproximadamente, em 2032, quando o subsídio será de 0,78125 BTC por bloco. Em 2140, aproximadamente, se não aumentarem as casas decimais, acabam os últimos *satoshis* de subsídio e o sistema terá que funcionar exclusivamente financiado por *fees*.

Os gráficos[340] seguintes de eixo radial e escala logarítmica plotam o preço do bitcoin dentro dos ciclos de 4 anos (cada ¼ de volta representa um ano) em US$ e ouro. O fato de a linha nunca ter cruzado demonstra que ninguém que tenha comprado e feito *hold* por 4 anos teve prejuízo nominal em *fiat*. Pelo contrário, em qualquer ponto analisado, o preço do BTC está a uma (10x) ou algumas (10^nx) ordens de grandeza maior do que no ciclo anterior. Se esse histórico for levado ao limite, ninguém que tenha feito *DCA* (compras parceladas recorrentes) por mais de 30 meses ou puro *lump sum* (compra de uma só vez) por mais de 40 teve prejuízo:

2010,'14,'18
gold price
10^14 (satoshi per ounce)
2009,'13,'17,'21
2011,'15,'19
2012,'16,'20
https://asset.gallery
license: CC BY-SA
updated: 2021-08-16

CAPÍTULO II: 10 OPERAÇÕES BÁSICAS - PRÓS, CONTRAS E CASOS

Existem basicamente três canais (*gateways*) para comprar bitcoin (análogas aquelas para comprar ouro): 1) Corretoras (*Exchanges* centralizadas e descentralizadas), 2) *OTC* (*over the counter*, mercado de balcão) e 3) *P2P (peer-to-peer* ou pessoa a pessoa, sem intermediários).

É possível adquirir bitcoins ou ouro por meio de aquisição original: mineração. Assim como, mendigando (*faucets*) ou sendo remunerado por algum serviço ou produto com esses ativos.

A melhor época para plantar uma árvore foi 20 anos atrás; o segundo melhor momento é agora. - Provérbio Zen

1) Mineração:

Consiste em ser remunerado por prover serviços de processamento de dados para *blockchain*. Forma de aquisição primária e original de cada bitcoin.

Hoje, essa atividade destina-se a grandes investidores, evitando a "maldição do vencedor", dispostos a converter grandes fluxos de *fiat* (moeda fiduciária) em *bitcoin* sem pressa, comprando serviços de grandes empresas.

Operam onde há energia a baixos valores: ociosa, isenta ou furtada[341], criando um mercado mundial de "valor-piso" da energia, subsidiando investimentos em produção, mesmo longe de centros consumidores industriais ou urbanos.

No início, mineração doméstica era viável, mas logo passou a ser dominada por agentes munidos de estruturas industriais com *hardwares* especializados.

Além disso, em muitos casos, a mineração é executada pelos próprios produtores dos *hardwares*, ou agentes com ligações próximas a eles, pois receber um equipamento depois de meses de seu lançamento já pode inviabilizar o retorno do investimento.

Devido às margens dependentes da cotação, alguns equipamentos se tornam obsoletos em menos de 16 meses. É um negócio de alta complexidade, investimento intensivo, alta dependência de acesso privilegiado e margens comprimidas.

Como não fazer[342]: se não tem equipamento, energia elétrica e banda de Internet a preços competitivos, terá prejuízo. Mineração na nuvem nunca foi viável, e mineração doméstica, sem furtar energia e obter *hardware* a baixo custo, não é viável desde a segunda Era de subsídio de mineração. Muitas vezes, a mineração é pretexto para venda de “pacotes” de lucro garantido em esquemas Ponzi.

2) Acumulação (*hodling/hodl*) e análise fundamentalista:

“Holdar" consiste em adquirir bitcoins como reserva de valor, mantendo suas chaves em locais seguros (como *paper wallets* geradas *off-line*, de preferência criptografadas). *Hodlers*[343] (acumuladores) limitam seu uso a alternativas com vantagens financeiras significativas, como envios internacionais, elisão fiscal, doações e pagamentos a dissidentes[344] e aquisição de *gifts cards*, para substituição imediata.

Destina-se a investidores de qualquer porte que avaliem que os ganhos e os riscos nas demais atividades não compensam o seu custo de oportunidade.

Como não fazer: Adquirir bitcoins e deixá-los em posse de terceiros (saldos em empresas) representa alto risco não remunerado, evidente em dezenas de casos de perdas (*MtGox*, *Bitfinex*, *Atlas* e outros). Vendendo acima de 35 mil reais por mês por CPF em corretoras brasileiras, sai-se da faixa de isenção e deve-se pagar imposto de renda (IN 1.888/2019[345]).

Resultados: Existem estratégias particulares a cada perfil na constituição de uma carteira: a) em todos os prazos significativos, quem adotou prática de preço médio (*DCA - dollar cost averaging*)[346] multiplicou sua riqueza se continuou por mais de um ciclo (4 anos), ressalvando que nas calculadoras de DCA não consideram outros ganhos – nem com *lending*, nem *trade* nem mesmo *forks*; b) quem tem experiência em operações em outros mercados, tempo livre e baixa aversão a risco pode bater retornos do mero preço médio fazendo capitalização por aluguel ou *lending* – ou alavancando por colateralizado de *fiat* inferior; c) para quem tem controle emocional para comprar caindo e vender subindo (o que é muito mais difícil do que pode parecer), adotando análises fundamentalistas, gráficas ou de sentimento – como *mayer multiple*, *S2F/S2FX*, dados *onchain*[347] ou *google trends* indicando buscas por bitcoin — há estratégias ainda mais lucrativas que DCA (que já não é *hodl*).

Também há estratégias que apresentam ganhos em USD (e, consequentemente, em *stables*) e em bitcoin sobre o simples *holding*, embora haja também trabalho e riscos marginais envolvidos.

Outras formas de análise de fundamentos mais elaboradas sobre o Bitcoin são: a) número de artigos acadêmicos escritos sobre Bitcoin que podem quantificar a penetração nas universidades; b) número de projetos de código aberto que contêm a palavra "Bitcoin" em repositórios de código como o *GitHub*, uma medida muito valiosa, pois demonstra a capacidade de cérebros desenvolvendo novas ferramentas e projetos complementares em torno da rede; c) dados *on-chain*, a principal fonte de dados para analisar os fundamentos de base, como poder de *hash* empregado pelos mineradores que protegem a rede, número de transações, dentre outras informações que podem ser encontradas em sites como *blockstream.info, coinmetrics, glassnode e skew.*

Satoshi Nakamoto, o primeiro bilionário pseudoanônimo nunca pagou impostos sobre sua fortuna, não investiu mais que seu trabalho e computação domésticos e esperou o patrimônio adquirido ganhar valor com o tempo.

3) *Trade* com análise técnica (AT)

Consiste em comprar e vender bitcoin por *altcoins*, *stable coins* ou *fiat*, segundo indicações de análise técnica (padrões gráficos, indicadores e osciladores). Destina-se a investidores com formação e experiência em AT – ou dispostos a desenvolvê-las com estudo – e que queiram aumentar lucratividade dedicando seu tempo e arriscando seu patrimônio.

Como não fazer: seguir esquemas de *pump and dump* como canais do *Telegram*, investir em *altcoins* sem ler a documentação básica e acompanhar as fontes de notícias, ou concentrar parte substancial da carteira na mesma corretora. A maioria das *altcoins* tende a virar pó. A maioria das corretoras que existiram deram *exit scam* ou foram supostamente *hackeadas*, algumas mais de uma vez.

Como fazer: Estude AT e inicie com trocados. Abra contas em diversas corretoras para diversificação e mantenha registros de sua contabilidade para controle. Só avance em complexidade dos produtos – mercados futuros, operações alavancadas e derivativos – quando compreender completamente suas consequências.

Negociar com bitcoins é altamente indicado para quem já tem experiência negociando ações, *forex* ou títulos, pois as regulações são muito menores e as variações são muito maiores – ampliando as possibilidades de ganho.

Os derivativos e *margin trade* são jogos de soma zero entre as contrapartes. Com os custos de transação, são jogos de soma negativa. Evite depositar valores significativos em qualquer corretora e depositar qualquer valor em corretora sem reputação.

Alavancagem é apenas indicada quando não tem liquidação forçada ou contra carteira diversificada, com a devida gestão de risco.

Estratégias com 100% de *TRACK RECORD* positivo até 2020:

Há estratégias com 100% de *track record* positivo em BTC e USD, tais como:

- Respeitar o múltiplo de *Mayer*, comprando abaixo de 200mma e vendendo acima de 2x200mma (Análise técnica);
- Comprar quando o *Google trends* indicar que expressões como *bitcoin* e *buy bitcoin* caíram abaixo de 50% da média e vender quando superarem 80%. Operar inversamente à manchete da CNBC teve 98% de acerto (Análise de sentimento);
- Comprar quando *hashrate* e número de transações por dia subirem sistematicamente e vender quando caírem (Análise fundamentalista).

4) Empréstimos p2p (*loan peer to peer*) e colateralizados

There is a war going on for ***your*** *bitcoins, and willpower is* ***your only defense****. Endless* ***Scammers*** *Everywhere. Bitcoin is a dangerous place.*

Os empréstimos pessoais (*p2p*) sem intermediação por empresa de crédito se iniciaram em plataformas como *btcjam*, *bitbond* e *bitlending club* em mercados insustentáveis (sem desenvolvimento de reputação entre partes) e colapsaram devido à ausência de colateral.

Empréstimos pessoais só são viáveis com *escrow* de confiança ou entre parentes: por exemplo pagando 2 ou 3x a sua mãe, avó ou tia o rendimento que ela tira no banco na perda fixa, dando a ela os bitcoins adquiridos como colateral.

O empréstimo de *fiat* colateralizado[348] em bitcoin é uma forma de consolidar renda em *USD/BRL* obtendo rendimentos superiores ao CDI, financiando a aquisição de bitcoins por juros inferiores aos cobrados pelos bancos pelo devedor.

Normalmente, quem contrai o empréstimo tem renda em *fiat* e deseja alavancar na aquisição de bitcoins, digamos, pegando R$ 200.000 emprestados a 2% ao mês. Se depois de 10 meses o preço do bitcoin aumentou 100%, o seu lucro na verdade foi 4000%, sendo que só pagou R$ 40.000 de juros e lucrou R$ 200.000.

Quem tem expectativa de hiperinflação em *rogue states*, Estados falidos, cada vez mais comuns, tem grandes resultados e motivações para alavancar em moedas locais. O ideal, muitas vezes, é obter alavancagem em fundos subsidiados (como venda de imóveis entre parentes, ou *lease back*).

Plataformas diversas como *Salt*, *Ethlend*, *Nexo.io*, *Celcius.network*, *Crypto.com, Binance, Blockfi e HodlHodl* também permitem empréstimos de dólares lastreados em criptos (e vice-versa), permitindo alavancagem.

A grande vantagem dessa operação é a elisão fiscal, uma vez que não há venda, não havendo fato gerador de imposto de renda, embora o investidor tenha acesso a dólares ou reais para pagar suas contas. A grande desvantagem é o risco de liquidação involuntária (*rekt*) se e quando o ativo dado como garantia (colateral) despencar de valor, abaixo do valor da dívida.

Negociar com empréstimos de bitcoins é altamente indicado para quem já tem experiência fazendo empréstimos e cobranças – especialmente com colateral e com pessoas com reputação, além das *DeFi*s (*decentralized finance*) e *CeFi*s (*centralized finance*).

Empréstimos colateralizados de *fiats* inferiores (como bolívar, peso argentino e real brasileiro) contra carteiras diversificadas (de bitcoins, com ouro, dólares e índices sintéticos de bitcoin, como DAI do *MakerDAO*) permitirão *bitcoiners (bitcoinheiros)* viverem perpetuamente como reis, comprando avião, iate e o que quiser sem pagar qualquer imposto de renda nem precisar comprar residência em Zug nem passaporte de St. Kitts, Vanuatu ou Antígua - porque empréstimo não é renda nem constitui ganho de capital.

Por isso se diz que logo você nunca precisará vender bitcoin, ele será como um título nobiliárquico que só é vendido quando a família já não tem mais nada.

5) Aluguel para margem (*lending for margin trade*)

Consiste em locação (*lending*) com intermediação por corretora (como *bitfinex*, *okcoin*, *blockfi*, *earn* e *poloniex*) ou para *traders* operarem *long* ou *short* – exatamente como aluguel de ações.[349]

Os saldos dos locatários são colaterais para pagamento dos locadores, havendo apenas risco de quebra ou incapacidade de execução da corretora.

Negociar com locação de bitcoins é indicado para quem pretende retornos entre 0,3% e 2% ao mês, suportando risco de custódia (insolvência das corretoras). Em especial, para quem buscar remuneração em *fiat* superior à das instituições de crédito convencionais e para quem pretende manter parte da carteira em *fiat* e parte em *cripto.*

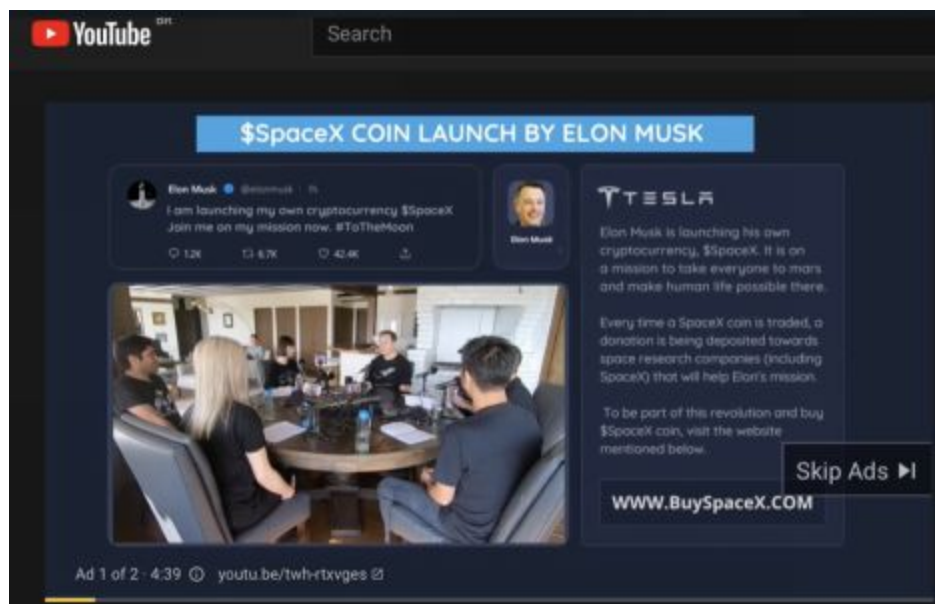
A utilização de *bots* (*software agents*) é muito comum tanto em *trades* quanto em *books* de aluguel. Em ambos os casos, recomenda-se leitura e estudo do seu funcionamento antes de colocar qualquer valor significativo. Se não forem usados *bots,* o aluguel pode demandar atenção diária para ajustar as ordens – altas o suficiente para dar algum retorno, mas baixas o suficiente para serem aceitas, não ficando com recursos parados.

Em geral, esse mercado gera diversas medidas relevantes. Quando o bitcoin está em tendência de queda, tende a ter remunerações maiores de aluguel; quando o bitcoin está em tendência de alta, geralmente a taxa para aluguel de bitcoin é mais baixa (e para aluguel de USD é mais alta).

Métricas[350] de mercado para medir otimismo são o *open interest* (total de contratos de derivativos em aberto que não foram liquidados); o percentual de ganho anualizado em fazer trava de bitcoin no mercado futuro (comprar bitcoin no mercado *spot*, presente; e, em sequência, vender futuro recebendo a diferença marginal como juro, remunerado em USD, ou vice-versa); e proporção de *shorts* e *longs* (indicando pessimismo ou otimismo).

Lending de *fiat* ou *stable fiat* (USDT, USDC, BUSD, por exemplo) também é uma forma de aumentar os saldos de quem precisa pagar obrigações nessas moedas, fazer *hedge* ou, simplesmente, “passar a chuva” esperando um momento de queda do bitcoin para recompra.

6) Pirâmides e *scams*, contos de fraudes

"Se você vê fraude e não diz fraude, você é uma fraude." - Taleb

Pirâmides são esquemas de remuneração de investidores pelo investimento de novos ingressantes, até colapsar quando não houver novos investidores suficientes, como a previdência obrigatória e insustentável de governo, como já foi demonstrado.

Casos famosos na comunidade brasileira de esquemas como este: *Anubis Trade*, *Atlas Quantum*, *Bitcoin Banco* (GBB), *Unick Forex*, *Dreams Digger Corporation* e vários outros.

Scam é uma expressão mais ampla que se refere genericamente à expropriação através de estelionato, até mesmo com *ICO* (*initial coin offering)* de criptomoedas inexistentes ou que não entregaram as funcionalidades anunciadas.

O mais comum atualmente é o pedido de depósitos justificados por hipotéticos *giveaway*: tipo, mande 1 bitcoin que vai ganhar 10, usando perfis *fakes* em redes sociais e impersonificação no *YouTube e até com contas oficiais do Twitter de personalidades como Obama, Biden, Musk e Buffet sendo hackeadas*[351].

Phishing é outra modalidade muito comum, em que domínios semelhantes a plataformas legítimas são criados e usuários que erram a digitação, ou os acessam por links anunciados em motores de busca ou mala direta, são induzidos a depositar saldos ou inserir senhas que deem acessos a saldos em sites de estelionatários. Isso também ocorre em sites de bancos e financeiras do *legacy* e demonstra que a cultura da criptografia e segurança da informação é, cada vez mais, essencial.

Outro golpe que chama a atenção pela ousadia e próximo ao *phishing* é a oferta de "falsas *wallets*" para *desktop* e *smartphones*, às vezes colocando até mesmo nas lojas oficiais de aplicativos os *softwares* falsos de estelionatários com nomes, símbolos, cores e tipografia semelhantes a produtos legítimos. Os incautos que não prestarem atenção e baixarem os referidos *apps* perderão os valores depositados, vez que acabarão por

revelar a *seed phrase* aos golpistas ou por criar carteiras a cujas chaves privadas eles já têm acesso.

Uma variedade de *scam* é o *exit scam* no qual os controladores das corretoras ou empresas fazendo custódia dos bitcoins simplesmente somem com os fundos dos clientes – normalmente, alegando que foram *hackeados* por terceiros desconhecidos e, em alguns casos, até simulando a própria morte (como alegado no caso da *exchange* canadense QuadrigaCX).

Há diversos golpes relacionados à manipulação de mercado, como divulgação de notícias e informações falsas ou sua manipulação (através de ataques de *spam* na rede aumentando *fees* e tempo de transações, ataques de *DDoS* tirando plataformas do ar); ou até mesmo por manipulação de preço para provocar liquidações involuntárias, para provocar *FUD* (*fear, uncertainty and doubt*) ou *FOMO* (*fear of missing out*); ou ambos, como nos esquemas de *pump and dump* que justificam a maioria dos grupos de "*calls* para trade", no *Telegram*.

Quem compreende que retornos são proporcionais a esforços e riscos compreende que promessas de retorno garantido "perpétuo de 3% ao dia" ou de "dobrar seus bitcoins semanalmente" claramente são mentiras e indicam evidências de crime.

Muitas pessoas têm seu primeiro contato com bitcoin caindo em golpes – e, na maioria das vezes, tornam-se *haters* depois do *rage quit,* porque a única maneira de reduzir a sua culpa e automartírio por causa da ingenuidade e perda de oportunidade é o bitcoin "morrendo". Isso ocorre devido às propriedades úteis do bitcoin, como relativa anonimidade. Pessoas livres aprendem com a experiência, perdedores culpam as sombras.

7) *Ransomware* (sequestro de dados)

As maiores mentes do mundo estão no Bitcoin, as maiores mentes criminosas também.

Consiste em espécie de *malware* que, após infectar o sistema, cobra "resgate" para que o acesso seja restabelecido. Em empresas com conteúdo de recuperação impossível ou inviável – como escritórios de advocacia –, muitas vezes a decisão de pagar a chantagem é inevitável[352].

Um caso de *ransomware* que popularizou o bitcoin foi o *wannacry*[353] em 2017. Diversos órgãos de inteligência acusaram que esse *malware* era um ataque norte-coreano[354]. Mesmo após a divulgação pública de que o pagamento não fazia os criminosos liberarem os dados, o golpe arrecadou mais de 50 bitcoins em 2017 (e continua arrecadando, como se pode conferir em seus endereços).

Muitas vezes, mesmo pagando o resgate, o código de desencriptação necessário para acessar os arquivos não são enviados. Esta possibilidade deve ser considerada na decisão sobre pagar ou não aos criminosos.

8) Arbitragem entre *exchanges* e moedas

Arbitragem é a operação praticamente simultânea em diferentes mercados, com obtenção de lucro, em teoria, sem risco, embora na prática existam riscos de *slippage* (diferença entre preço esperado e real, muitas vezes devido a sua própria ação em ordens ativas mudando cotação) e de solvência das plataformas (risco de custódia), como qualquer operação em plataformas centralizadas ou descentralizadas.

Arbitragem entre *exchanges* (corretoras) é possível quando são identificadas diferenças de valor que compensem os custos de transação. Como a mineração é inviável no Brasil, pode-se supor que quase todos os bitcoins em circulação foram "importados" por este processo.

As diferenças de preço (*spread*) entre corretoras de outros países apresentam variações ainda maiores. Assim, o ágio (*spread*) indica a dificuldade de fazer remessas internacionais. Nesses casos, lucra quem pode fazer envios internacionais com baixo custo – seja usando plataformas como *Zro Bank*, *Wise (antiga TransferWise)* ou remessaonline.com.br, seja levando dinheiro fisicamente ou tendo facilidades, como as oferecidas pelo BB Americas, XP investimentos ou outros bancos comerciais a alguns clientes.

Caso a compra e a venda não ocorram simultaneamente, há o risco de "*slippage*" – que a variação na cotação destrua a margem de lucro. O ágio do bitcoin no Brasil tem caído sistematicamente, reflexo da base consumidora deste mercado, que tem aumentado exponencialmente.

9) *Bounties* e novos serviços

"Novos serviços no ecossistema" podem ser: suporte operacional, técnico ou de desenvolvimento, como colaborador independente: *Bitrefill*, bitmilhas, p2p. Advogados, contadores, designers, programadores especializados são altamente demandados.

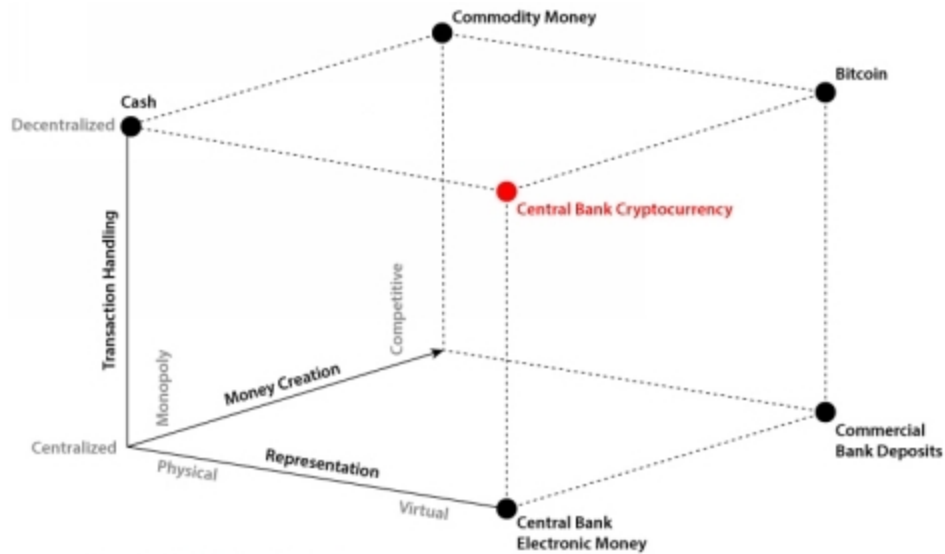
Depois que o ecossistema atingir certa massa crítica, as pessoas que não tiverem as habilidades para utilizá-lo ficarão obsoletas. Pode ser desenvolvendo aplicativos ou comprando e vendendo bitcoin na vizinhança usando *network* orgânico ou na gestão de redes sociais, a demanda por estes profissionais é maior que a oferta.

As habilidades necessárias para oferecer serviços no ambiente dependem de educação real – que é o oposto ao que é oferecido na instrução formal – e isso demanda assunção de riscos e esforços.

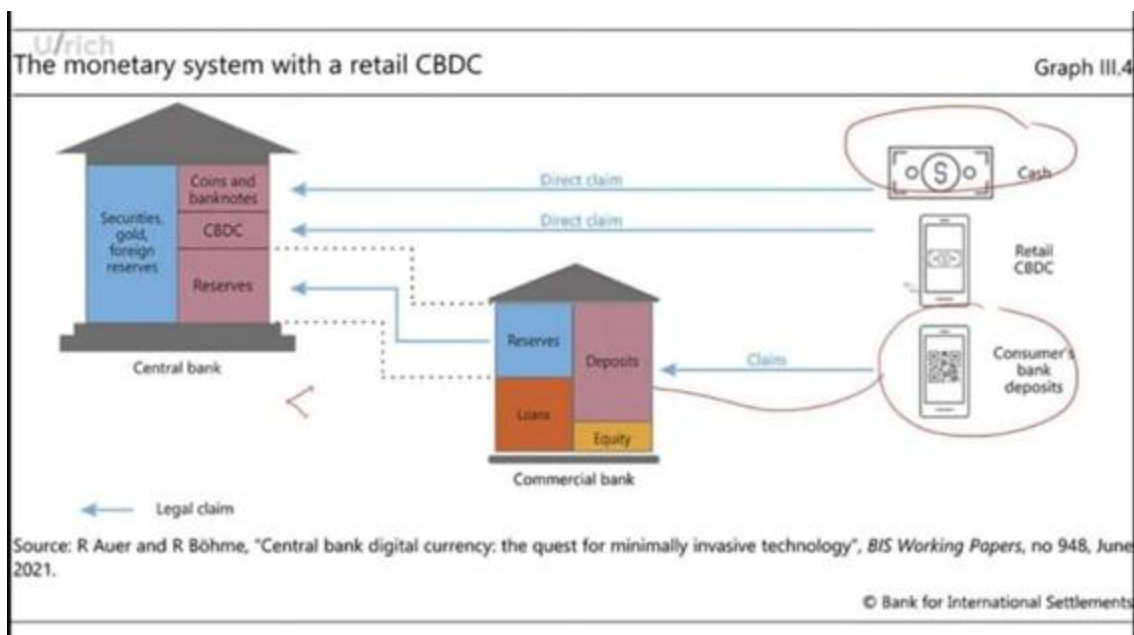
Bounty é espólio, butim, normalmente prêmio feito como: divulgação por *referrals* de indicação de inscrição em plataformas, remuneração de c*ommunity managers* (com serviço de suporte, produção de vídeos e divulgação em redes sociais), a descoberta ou correção de *bugs* e falhas de segurança em plataformas e até em *blockchains*.

9.1) O novo serviço problema: CBDC's

Os bancos atualmente são a antítese do capitalismo. A deterioração do *Deutsche Bank* e do sistema bancário europeu é evidência do esquema insustentável a que são submetidos. A sua chance de sobrevida virá da "Guerra ao dinheiro", das tentativas de limitar ou eliminar o dinheiro físico (implantando o controle totalitário sobre as finanças), como nas CBDCs[355].

Figure 1: Control Structure of Currencies
NOTE: Figure 1 is adapted from Berentsen and Schär (2017).

As CBDCs[356] não são semelhantes a criptomoedas, são seu exato oposto: totalmente centralizadas, vulneráveis a expropriações voluntárias, violações de privacidade, mudanças de regras sem consenso; e, a diluição por senhoriagem[357]:

As CBDCs – *Central Bank Digital Currencies* (moeda digital de Banco Central) aumentam brutalmente o poder dos governos, inclusive sobre os bancos, uma vez que o próprio banco central vai processar as transações (como no PIX) e manter registros de todos os saldos. Estudos da ONU e do FED indicam que as CBDC’s poderiam matar os bancos comerciais e que a próxima etapa da “*FED Coins*" seria o “*FED APP"*, dispensando a intermediação bancária[358].

O fim dos bancos como conhecemos:[359]

Quanto mais agressivas forem as tentativas de expropriação de bens[360], imposição de sistemas de créditos sociais para acesso a negócios ou serviços; e, criminalização/restrição de atividades econômicas negras e cinzas[361], maior será a demanda por alternativas.

Como vão operar camelôs, indigentes, traficantes, profissionais de saúde que operam sem recibo, GPs, políticos comprando votos e o jogo do bicho - apenas como exemplos rotineiros - com o fim da moeda alodial? Vão pagar no PIX? Vão voltar a usar ouro e prata? Ou vão desistir das atividades informais e ilegais? Você tem as ferramentas e conhecimento para certificar a pureza de ouro ou prata? Acredita que a banca de jogo do bicho terá?

9.2) As soluções: uberização e empreendedorismo

Uberização é o processo de criação de valor em intermediação provendo ambiente negocial com algum grau de segurança entre partes, oferecendo plataforma em que serviços e produtos são ofertados e aceitos com sistemas de reputação e *escrow* - como *Uber*, *Airbnb*, *iFood*, *Silk Road* e *Bisq*.

Dezenas de bilhões de dólares estão sendo investidos em *FinTechs* (como *Circle*, *Uphold*, *Bitpay* e as diversas empresas mencionadas). Os bancos e demais instituições financeiras não têm expectativas positivas com juros sistematicamente negativos e crescente competição de serviços que não estão submetidos a suas regulações extremas.

Não foram apenas entes de reputação e legado superiores, como Satoshi, que ficaram bilionários empreendendo no ecossistema, também há figuras abjetas como Vitalik (*Ethereum*) e Roger Ver (*Bitcoin Cash*), além de outras controversas - como Changpeng Zhao (*Binance*), Sam Bankman-Fried (*FTX*) e os irmãos Winklevoss (*Gemini-Blockfi*) nesse *ranking*. Um exemplo de empreendedor controverso (já preso, inclusive) que produz conteúdos de altíssima qualidade é o Arthur Hayes, da *Bitmex*[362].

As oportunidades são amplas e a disponibilidade de investimentos por *private equity* e *venture capital* é crescente.

Os riscos do pioneirismo são altíssimos. Centenas de *altcoins* viraram pó, não tendo mais negociação em qualquer corretora. Várias empresas no ecossistema foram *hackeadas* e faliram.

A infraestrutura básica mudou em cada Era:

1) (2009-2012): repositórios para *download*, fóruns, *faucets*, *exchanges* estáticas[363], *mineração com GPU/FPGA e* apostas simples aleatórias, com oráculo *onchain*, como *satoshidice*[364];

2) (2012-2016): corretoras com *fiat, stables* e *margin trade, sites* de notícias e relatórios especializados, plataformas de apostas multilaterais de eventos como bitbet.us, *ATM*s de BTC e mineração com *ASICs*;

3) (2016-2020): *DeFis, exchanges* com sintéticos (negociando futuros e derivativos, como *Bitmex* e *Deribit*), plataformas de empréstimos colateralizados (viabilizando consumo legal sem imposto de renda e alavancagem, como *Nexo*, *Blockfi* e C*elcius*), de trocas *offchain* (saldos entre clientes) e 2ª camada (*Lightning*), *Sidecahins*, *DLCs* e *gateways* alternativos (cartões pré-pagos e *marketplaces* de milhas e *gift cards*), *air-gapped hardware wallets* (carteiras *offline* sem contato físico com terminais)[365].

4) (2020-2024) *ETF*s e fundos de BTC, facilitando acesso institucional sem risco de custódia, plataformas de serviços financeiros completos - que além de *margin trade*, opções e futuros, ofereçam colateralizados contra carteiras múltiplas, *copy trade* substituindo "gestor profissional", capitalização passiva de saldos com *bot* alocando em *cash and carry*, *lending* ou empréstimo; e, tokenização de índices, ações, moedas e *commodities* (sintéticos colateralizados em BTC ou lastreados em saldos da plataforma) que possam ser negociados 24/7 (tornando corretoras convencionais de ações obsoletas); e, tokenização de apostas de eventos negociadas em *books* como os *tokens* TRUMP2020, TRUMP2024 ou BOLSONARO2022[366] na *FTX*. *Wallets* que integrem funções de *chat* com transações em diversas camadas - como a *Zebedee* com *Discord, Status, Alipay e WeChat*. Plataformas de *podcast* com remuneração direta aos produtores de conteúdo via soluções de segunda camada, como *Breeze* e *Sphinx*.

5) Na 5º Era (2024-2028), a tendência é que as *wallets* interajam além de transações em várias camadas e serviços de *chat*, oferendo outros serviços de comunicação e privacidade (como *VPN*, compartilhamento remunerado de banda, capitalização e colateralizado sem intermediários e oferta ou aceitação de serviços e produtos "uberizados"). Neste período, as plataformas

> sobreviventes devem ampliar os serviços oferecidos e, após substituir bancos e corretoras de valores, passem a substituir também loterias, seguradoras e, finalmente, a justiça estatal com serviços de apostas decentralizadas de morte e decisões decentralizadas de conflitos[367].

Durante as 4ª e 5ª Eras será esperado que a maioria das corretoras que dependam de serviços bancários em países bolivarianos sejam eliminadas (criminalizadas ou inviabilizadas por regulamentações) ou capturadas (adquiridas por cantilionários amigos do rei). O sistema bancário convencional será brutalmente impactado por *CBDCs* e *APPs* de bancos centrais, até mais do que já sofreu na última década com as *fintechs* e o juro negativo. Após os Bancos Centrais serem responsáveis por processar a maioria das transações (como no PIX), eles tenderão a oferecer plataforma oficial para pagamentos e capitalização (estatal ou de empresa com controladores ligados intimamente a governo[368]), eliminando a necessidade de intermediários bancários – facilitando ainda mais a manutenção de juros reais negativos.

Cada etapa dessa guerra apresentará novas e enormes oportunidades aos emprendedores.

Hal Finney
"Running Bitcoin"
(Twitter)

Arte de comemoração ao 10º aniversário de Hal Finney *'Running Bitcoin'*.
(10 de jan de 2009) / **Fonte:** Cryptograffiti (artist)

Roteiro passo a passo para comunidade *bitcoiner*:

1) Estude, com ceticismo, *Twitter, Bitcointalk, Discord, GitHub e Reddit*, que são os lugares onde se concentram as principais discussões *crypto*[369]. A maioria das comunidades abertas do Facebook e propagandas do YouTube são antros de criminosos ou pura desinformação. Acompanhe os *meet ups* locais.

2) Cadastre-se nas plataformas nacionais (*Walltime, Rispar, Foxbit, Biscoint, Bipa.app*), pesquise quem vende ou compra a melhor preço no biscoint.io antes do depósito e não venda mais de

R$ 35 mil por mês por CPF em corretoras nacionais, se não quiser pagar imposto;

3) Acompanhe as comunidades internacionais (*reddit*, *bitcointalk*, IRC WOT); e os canais do *YouTube* e livros de "evangelistas" como Bitcoinheiros, Andreas Antonopoulos e Saifedean Ammous; e podcasts, como Stephan Livera e Jimmy Song;

4) Abra conta nas corretoras estrangeiras com reputação e tenha intimidade em usar plataformas — fornecendo apenas *email* de *small tech*[370]. que valorize privacidade e não exija dados pessoais. Nunca use para nada de relevante *e-mail* de *big tech*. Essas podem fornecer *master keys* a governos totalitários e policialescos[371] e usar seus dados para reduzir seu "extremismo" usando técnicas de "desradicalização"[372] por *nudging*;

5) *Exchange* (corretora) não é carteira. Utilize para guardar seus bitcoins apenas soluções como *paper wallets* geradas *off-line* e criptografadas, com *passphrase* (para os mais avançados); *Wallet mobile* (para pequenas quantias e de preferência que use *Lightning Network*); e *Hardware wallets* (para uso constante, sem depender de uso de navegadores, com recursos como *multisig*);

6) Utilize, após referências e pesquisas, demais empresas e serviços do ecossistema – *Fold*, *Bitrefill*, *Glin*, *Celsius network*, *NEXO*, *BlockFi*, *Crypto.com*, *Hodlhodl*, *LocalBitcoins e* opções descentralizadas como a *Bisq*;

7) Seja feliz com sua independência.

O que foi mencionado até aqui é o presente e o básico, agora se quiser aprofundar e vislumbrar o futuro, continue.

Bitcoin Memes – "Estou aqui pela tecnologia."

CAPÍTULO III:
PERSPECTIVAS FUTURAS E AMEAÇAS

1) É bolha?

É importante refutar o mito repetido de que “bitcoin é bolha”. Na verdade, o bitcoin é a agulha que pode estourar “a bolha de tudo”[373] (*the everything bubble*) criada pelo juro negativo, com governos comprando trilhões em ativos a qualquer preço e mantendo vivas empresas zumbis (cujo faturamento é insuficiente para pagar os juros das dívidas).

Robert Schiller, prêmio Nobel e docente de um curso gratuito de finanças no *Coursera*[374], nas edições mais recentes de seu livro *Irrational Exuberance*, afirma que “o maior exemplo de bolha da atualidade é o bitcoin”.

Bolha econômica ou de ativos, bolha de mercado, bolha especulativa ou bolha financeira são sinônimos e descrevem a situação em que o preço de um ativo se descola do seu valor fundamental. Um critério objetivo para a sua definição é quando o preço de um ativo sobe mais que dois desvios-padrão.

Isso ocorre ciclicamente no BTC, devido aos processos de *FOMO* (*fear of missing out*), normalmente no ano imediatamente posterior a cada *halving*, logo depois corrigindo (também seguindo padrão emocional, *FUD* (*fear uncertainty and doubt*) para recomeçar o ciclo. Como o Bitcoin tem fractal próprio, em decorrência dos choques de oferta nos *halvenings*, ele ciclicamente entra em “bolha” quando seus retornos médios ultrapassam o dobro do seu desvio-padrão.

Adotando a definição de bolha baseada em análise técnica (bolha a partir da variação superior a dois desvios-padrão), o bitcoin passou por quatro bolhas: 1) de abril até junho de 2011, de 0,31 para 31 USD; 2) entre dezembro de 2012 e abril de 2013, de 13 para 266 USD (Crise cambial do Chipre); 3) de junho a novembro de 2013, de 100 para 1.300 USD; e 4) de abril a dezembro de 2017, indo de 1.200 até 19.700 USD[375].

Em cada uma dessas oportunidades, nas quais multiplicou de valor 100x, 20,5x, 13x e 14,91x, existiram correções equivalentes e subsequentes

períodos de acumulação – exatamente como previsto na Teoria das Ondas (de Dow e Elliot) e nos seus “Ciclos emocionais de mercado”.

O preço do bitcoin passou por bolhas e tende a passar por outras mais, quando seu preço aumentar mais de 10x em poucos meses. Porém, em sua tendência normal de aumentar no ritmo do aumento de sua base de usuários, não se pode afirmar que seja bolha, mas apenas consequência da Lei de Metcalfe[376] e curva normal de adoção de tecnologia, a não ser que razões políticas ou técnicas indiquem perda de valor fundamental.

Em termos fundamentais, bolha é quando o preço descola dos seus parâmetros de precificação.

Razões políticas podem mitigar o valor fundamental do Bitcoin. Se os principais governos mundiais voltarem ao padrão-ouro com conversibilidade integral, se os principais governos do mundo funcionarem em superávit (arrecadando mais do que gastam), se forem revogados todos os controles de capitais, tributos e expropriações involuntárias, assim como as limitações para o comércio e o investimento globais, aí, sim, o Bitcoin poderá perder grande parte de seu sentido, sua base de usuários e seu valor fundamental.

Interessante notar que as experiências de proibição e criminalização das operações com criptomoedas não resultam em redução do seu valor na respectiva jurisdição – pelo contrário, exatamente como a proibição das drogas ou do álcool, passa a haver ágio.

Razões técnicas também podem mitigar o valor fundamental do Bitcoin, tais como: 1) se houver queda significativa do *hashrate*; 2) se uma quantidade significativa de desenvolvedores abandonarem o projeto (ou forem presos ou mortos); 3) se uma quantidade significativa de *tokens* for apropriada por entidade disposta a vender por qualquer preço, como aconteceu com a massa falida do *Mt. Gox* e a *Tokyo Whale*; ou 4) se o sistema sofrer ataques significantes, como os ataques de *spam* dos mineradores em 2017, que encareceram as *fees*.

Até que ocorra o fim (ou irrelevância) dos governos como conhecemos, é crível que as razões políticas venham a mitigar o valor do Bitcoin.

Bitcoin Memes

"A questão não é quanto alto pode ir o Bitcoin, mas, sim, quão baixo pode ir o dólar. Se o dólar for a zero, o valor relativo do bitcoin será infinito…"

1.1) Qual o valor de uso do bitcoin?

Serve para fazer remessas internacionais independentemente de controles de capitais, para garantir imunidade contra tributos e execuções involuntárias em face de ditaduras e perseguições institucionais, e serve como reserva de valor pseudoanônima imune a diluição de moedas e de políticas governamentais.

Quanto maiores os tributos, quanto mais absurdas as regulações, quanto maior o *déficit* e maior a dívida pública, quanto mais numerosos forem os embargos e controles de capitais – mais útil será o Bitcoin.

É uma hipótese plausível e corrente na comunidade que, se os governos tivessem mantido o padrão-ouro, com conversibilidade integral, o tamanho dos Estados teria permanecido limitado; e, provavelmente, o Bitcoin nunca teria sido criado; e, se fosse, não teria se popularizado.

Dessa forma, o Bitcoin foi criado em decorrência do abuso de poder e corrupção extrema dos governos – como repetidamente confirmado por Satoshi até mesmo no Bloco Gênese ao escrever o texto *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*. Assim, quanto maior o descontrole e o abuso governamental, maior deve ser o valor fundamental do Bitcoin.

The Times de 3 de janeiro de 2009. O Bloco Gênese deixou uma mensagem, a qual faz referência a esse jornal. Atualmente, um exemplar dessa edição vale milhares de dólares e é objeto colecionável.

THE TIMES

£1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Israel prepares to send tanks and troops into Gaza

Michael Sheen
Frost, Nixon and me

Working mums
So that's how she does it

Detox in style
The best spas on the planet

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

Salman Rushdie
I won't marry again

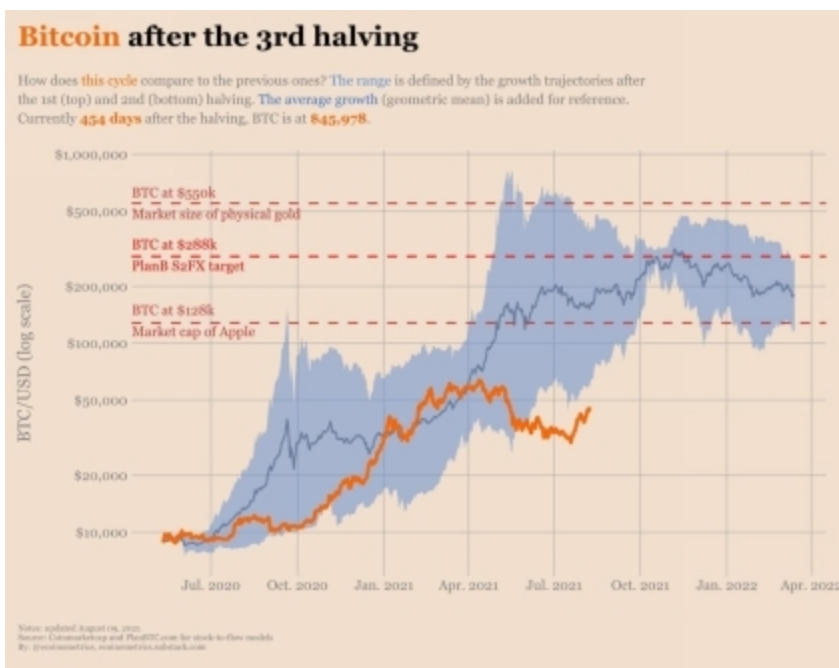
Giant killing?
Guide to the FA Cup third round

O valor das dívidas corporativas globais é exponencial, assim como as limitações quanto às liberdades individuais e a ampla consciência de que o sistema em que vivemos é inevitável – como popularizado por Peter Schiff e Mike Maloney, além de outros expoentes da Escola Austríaca. É isso que alimenta a tendência exponencial, desde 2010, do valor do bitcoin.

A primeira definição é mais complexa de classificar, pois o valor fundamental do Bitcoin (como de qualquer criptomoeda) é subjetivo e depende de obtenção de dados estimados (e não objetivamente calculados), como número de usuários, velocidade de circulação, *proof of brain* (captação relativa de cérebros), *proof of stake* (captação de investidores relevantes), *proof of work* (capacidade computacional dedicada) e até mesmo a qualidade das contribuições no seu repositório e das empresas no seu ecossistema – há uma série de artigos de alta complexidade sobre o tema.

No canal Aimstone do *YouTube*, há um episódio de 2018 muito didático explicando a estimativa de US$ 1,2 milhão por bitcoin como valor alvo, por uma lógica simples: nos anos anteriores, o aumento no número de carteiras era proporcional ao aumento de preço (ambos multiplicaram 20x); então, assumindo como limite de crescimento algo em torno de 2,4 bilhões de usuários (todas as pessoas entre 18-64 anos com acesso à *Internet* e a *smartphones*) o aumento dos atuais 20 milhões para 2,4 bilhões de pessoas ocorreria, seguindo a taxa atual de adoção, em 4 a 7 anos. No mesmo canal, a estimativa mais atual[377] é de US$ 12,5 milhões de dólares por bitcoin em 2031.

Valuations lineares são comuns, até mesmo no relatório de Ray Dalio, existem as estimativas de preço para os cenários que o bitcoin ficaria com x% do mercado do ouro, y% dos mercados de remessas e z% dos mercados de ações e imóveis. O problema com essas estimativas é que a base de cálculo (riqueza mundial) não é estanque, de modo que, quanto mais pessoas adquirem o bitcoin, mais riqueza é gerada com mais liberdade econômica e menos riqueza é destruída por distorções derivadas do juro negativo e totalitarismo.

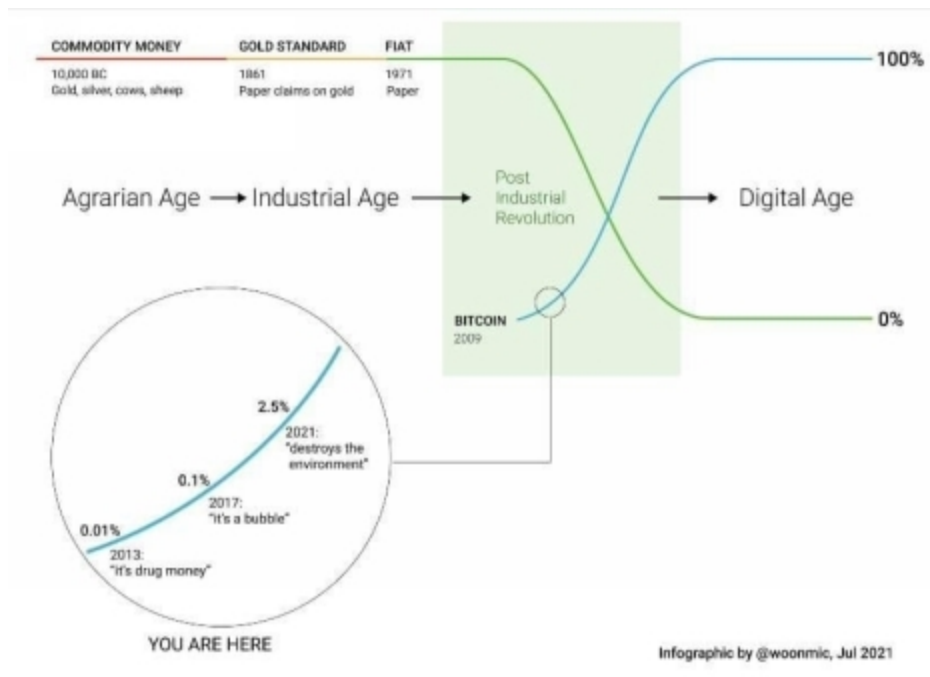
Dizer que o bitcoin precisa valer valer 550k USD para bater o *market cap*[378] do ouro não diz muito, até porque há quem[379] defenda que XAU (31,1 g) pode valer US$ 50 mil em 2022, com a volta do *gold standard:*

A questão é um pouco mais complexa, pois estão sendo desenvolvidos produtos financeiros que permitam a instituições investirem em bitcoin sem o risco de custódia, com destaque para *Fidelity, Grayscale, Purpose e Bakkt*. Como a maior parte dos recursos nos mercados pertencem a instituições e não a pessoas físicas, a projeção mencionada já perde o sentido.

Se o BTC avançar segundo as cinco fases de Barry Silbert[380], a quarta fase (atual) é a adoção institucional (compra por corporações fundos e investidores institucionais por meio de ETFs) e a próxima (5ª fase) será quando órgãos governamentais (Bancos Centrais) e supranacionais vão competir adquirindo bitcoin (primeiro como reserva, depois como lastro de moeda; e, por fim, como moeda) – seja comprando a mercado ou desapropriando bitcoins de seus cidadãos (como Andreas Antonopoulos teme que ocorra com eventual *ETF*). Outra maneira de governos acumularem bitcoins é parando de leiloar os bitcoins apreendidos – como o governo norte-americano faz constantemente.[381]

Para o venezuelano cuja alternativa à criptomoeda é acumular bolívares, que perdem metade do valor a cada 18 dias; para o trabalhador ilegal em países de economia desenvolvida, que precisa mandar recursos para sua família também desbancarizada no interior de jurisdições de economia subdesenvolvida; ou, para o empresário que quer pagar certa comissão

ilegal que, se for rastreada, resulta em cadeia (como Eike Batista foi preso), as criptomoedas podem ter valores utilitários peculiares.

Agregar as demandas mencionadas apenas em DeFi (protocolos de finanças alegadamente descentralizadas) é uma tarefa improvável. Os mercados descentralizados podem ser oferecidos por redes federadas (como *Liquid*) ou de 2ª camada (como *Lightning*) de maneira mais barata, rápida e segura que *blockchains* marginais. Talvez o mercado de *smart contracts* seja perpetuamente algo de nicho e talvez substitua grande parte do mercado CeFi (financas centralizadas), em todo caso, a participação do bitcoin nesses mercados tende a ser crescente com diversas atualizações aumentando sua fungibilidade, escalabilidade e funcionalidade, como o *Taproot (BIP341)* e posteriores:

Tendências de Migração das Riquezas

O ecossistema de criptomoedas mostra como funciona o livre mercado real. Mesmo com proliferação de crimes e manipulações — como aquelas relacionadas a emissão de USDT[382] (por inexistência de colateral ou colateral sem qualidade) e as decorrentes dos mercados futuros[383] na *CME/Bitmex/Deribit/LedgerX/Bakkt* para provocar "*maximum pain*[384]" nos mercados de opções — o mercado se autorregula de maneira anti-frágil, se aperfeiçoa pelo aprendizado e ninguém recebe *bail-out* mesmo com quedas de mais de 90% das cotações de mercado.

A liberdade suprema leva à responsabilidade extrema. No Bitcoin não há como mudar as regras no meio do jogo, como acontece no Ethereum.

Estimativas mais simples do valor fundamental do Bitcoin são feitas a partir da consideração de quanto dos mercados existentes ele pode ocupar – por exemplo, se o Bitcoin tomasse metade do mercado do ouro[385], valeria mais 6 trilhões em *market cap* (US$ 330 mil por bitcoin com ouro a US$ 1.900); se o bitcoin ocupasse 20% das *offshores* em paraísos fiscais, abocanharia mais 7 trilhões de dólares; e assim por diante, em mercados de remessas; *black* e *gray markets* (como tráfico de drogas, armas, escravos, corrupção e descaminho); e até os mercados de ações (US$ 120 trilhões), *fiats* (US$ 110 trilhões) imóveis (US$ 300 trilhões), dívidas (US$ 300 trilhões) e derivativos (entre 0,6 e 1 quadrilhão de dólares) que tendem a perder um percentual de seus investidores para o Bitcoin.

O PIB global foi de 88 trilhões de dólares em 2019 (mais que o dobro daquele de 1990). A criação e acumulo de riquezas são exponenciais – e só perdem para o ritmo atual de aumento de dívida e impressão de moedas fiduciárias.

Para se ter uma ideia do quão irrelevante ainda é o mercado de bitcoins (embora já tenha superado o *market cap* da prata), pode ser demonstrado que, segundo compilação da *visualcapitalist*[386], existiam mais de 2.100 indivíduos bilionários (com patrimônio médio de mais de 8 bilhões cada); mais de 13 milhões de *HNWI (High Net Worth Individuals*, com patrimônio líquido de mais de US$ 20 milhões); e, mais de 50 milhões de milionários (em patrimônio líquido em dólar). Isso era em 2020, agora é muito mais.

Assim, a riqueza privada formal do mundo é estimada em mais de um quadrilhão de dólares, se forem somados os ativos públicos e mercados negros e cinzas, deve ser muitas vezes mais.

Se as taxas de inflação do ouro[387] mantiverem sua tendência histórica[388], nunca haverá mais que 1 bitcoin para cada 10 quilos de ouro (199M kg/19M BTC > 0,1 BTC por kg). Retirando daí os bitcoins perdidos (já que as reservas de ouro não contam ouro no fundo do mar), seriam 12 a 13 kg de ouro por BTC[389] (em agosto de 2020 avaliados em mais de 4 milhões de reais).

Com o total de 8 bilhões de pessoas no mundo[390], seria: 21M/8B = 0,002625 BTC por pessoa; e, 21M/50M = 0,38 BTC por milionário. Isso considerando a emissão máxima final a ser atingida em 2140, se formos subtrair os milhões de bitcoins perdidos e milhões ainda não criados o valor ainda seria 30 a 45% menor. Se bitcoins ainda existirem em 12 anos, serão mais escassos que imóveis ou qualquer outra classe de ativo, como demonstrado no S2FX.

São emitidos apenas 900 novos bitcoins por dia, na Era atual[391]. É quase impossível que uma entidade (mesmo governamental) que comece a comprar agora consiga captar a mercado mais que os 654.885 sob custódia da Grayscale[392] ou que uma corporação acumule reservas[393] superiores a Microstrategy (105.085 BTC) e Tesla (38.300 BTC)[394], se os últimos não forem desapropriados ou venderem de maneira relevante.

Todo bitcoin tem um preço, mas a maioria deles não esta à venda por *fiat*, mas por liberdade – território soberano, passaportes com isenção perpetua de tributos e realização de sonhos.

Se mais de 86% não venderam seus bitcoins na queda, em 2018, de US$ 19.500 para menos de US$ 3.500, quantos venderão facilmente quando vier a hiperinflação em *fiats*? É a "minoria intransigente”de Taleb.

Revista Veja, dezembro de 2017.

NEGÓCIOS

Grupo Abril é vendido por R$ 100 mil para especialista em aquisição de empresas quebradas

Por R$ 100 mil, o empresário Fábio Carvalho comprou a Abril, assumindo os R$ 1,6 bilhão de dívidas que causaram o pedido de recuperação judicial

Em alguns anos, um exemplar destes valerá mais que a Veja (empresa com todos os ativos) em um leilão de colecionáveis. O grupo dono da VEJA foi vendida em 2018 por 100 mil reais - provando que "você pode ignorar a realidade, mas não as consequências dela".

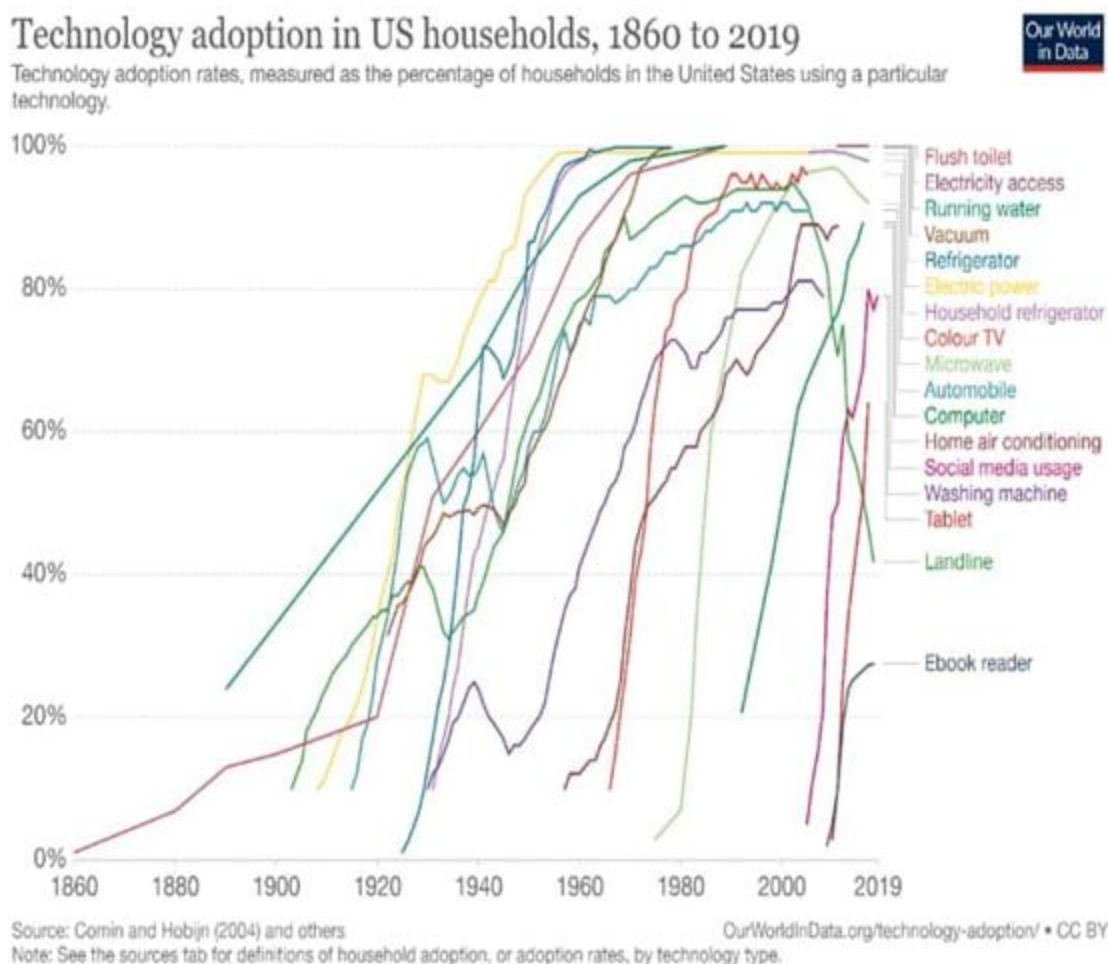
Uma coisa é certa: quando aprenderem a operar criptomoedas, nunca mais petistas precisarão viajar com dólares na cueca, nem amante de presidente levar dezenas de milhões de euros no avião presidencial, nem peemedebista baiano alugar apartamento para servir de depósito de dezenas de milhões de numerário em espécie; e, muito menos, senador bolsonarista vai precisar ser humilhado com a polícia tirando 30 mil reais de seu traseiro com resíduos de fezes (episódio que deu outra dimensão ao conceito de "dinheiro sujo"). Também neste aspecto, o Bitcoin é o dinheiro mais limpo já criado.

Se a população do planeta não for agressivamente destruída, nunca existirá nem 1 bitcoin para cada 420 pessoas. Por esses motivos, acredita-se que, no futuro, os preços serão expressos em satoshis, se o bitcoin atingir a fase 5.

Há projeções que indicam que, se a taxa de adoção e o aumento de preços exponenciais forem mantidos, em 10 anos, as criptomoedas tenderão a sugar o valor hoje circulando em moeda fiduciária estatal (US$ 100 trilhões, em dezembro de 2019). Isso não será o fim das *fiats*, mas o fim de sua significância. Elas podem continuar existindo, como hoje existem as indústrias de selas e de lampiões – embora sejam objetos obsoletos.

A questão é que o bitcoin, ao valorizar 100x, cria riqueza e propicia negócios e eliminação de perdas como *malinvestments*, de modo a aumentar a riqueza total.

Existem dois porquês pelos quais o valor do bitcoin pode subir exponencialmente – ao contrário do valor de ações e de outros ativos limitados a fluxos de caixa de negócio ou bens físicos: 1) a Lei de Metcalfe enuncia que o valor de conexão em uma rede é proporcional ao quadrado do número de participantes: quanto mais pessoas tiverem bitcoin, mais fácil será encontrar pessoas que o negociem; quanto mais dinheiro for investido no ecossistema, dado que sua oferta é predeterminada e não pode ser inflacionada, maior o valor que o *token* poderá alcançar; e 2) sua oferta tem inflação decrescente, mesmo que a demanda seja constante, a sua oferta

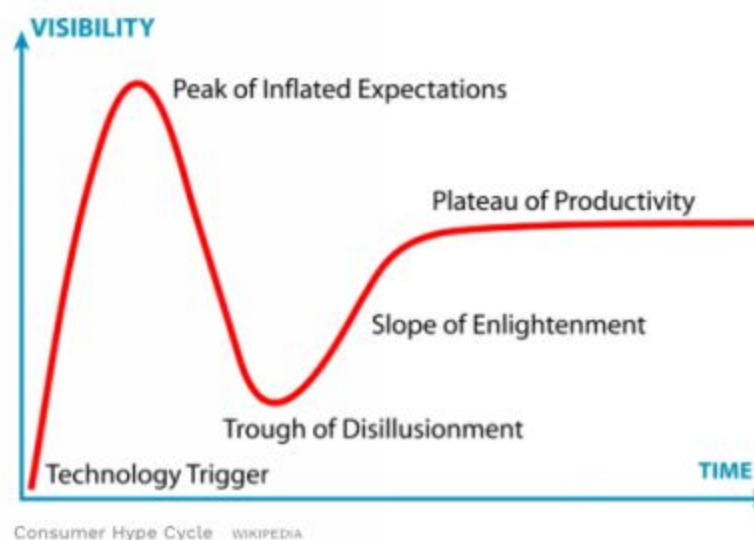
marginal é decrescente – isso sem considerar os bitcoins perdidos – também em decorrência da Lei de Metcalfe, o valor de tecnologias adotadas geralmente aumenta de maneira exponencial até atingir um platô e estabilizar. O gráfico seguinte mostra a “curva S” para várias tecnologias:

Tendemos a superestimar o efeito de uma tecnologia no curto prazo e a subestimar seu efeito no longo prazo.

Roy Charles Amara

Este fenômeno é conhecido como Lei de Amara:

2) Ciclo de hype da tecnologia: Gartner Hype Cycle

O *Gartner Hype Cycle* é uma metodologia que oferece uma visão de como uma tecnologia ou aplicativo evoluirá ao longo do tempo, fornecendo uma fonte sólida de insights para gerenciar sua implantação dentro do contexto de seus objetivos de negócios específicos. O ciclo fornece uma representação gráfica da introdução, maturidade e aceitação de novas tecnologias.

De acordo com alguns analistas *bitcoiners*, o Bitcoin pode estar oficialmente entrando no *"Slope Of Enlightenment" (figura anterior).* A "inclinação/tendência" é uma das etapas de um ciclo tecnológico descoberto pela empresa líder em pesquisa e consultoria Gartner, o *Gartner Hype Cycle*[395]:

Com esta ferramenta metodológica, executivos, investidores, *traders* e pesquisadores possuirão a capacidade de filtrar o ciclo de FUD/FOMO na adoção de tecnologias. Por isso que é a metodologia que ajuda a entender o processo de maturidade e adoção das inovações.

Uma compreensão adequada do ciclo de hype permite que os investidores reduzam e aumentem o risco e aumente lucratividade, operando do lado oposto das falhas emocionais. Essa mesma fonte, afirma que o Bitcoin pode ter já passado pelo "Vale da Desilusão" e agora estaria entrando na fase de "esclarecimento" (*Slope Of Enlightenment*).

3) Adoção, volatilidade e hiperbitcoinização

“Reclamar que bitcoin é volátil é como
reclamar que o céu é azul.”

Hiperbitcoinização é o momento em que o BTC não corrige mais em *fiat* e ninguém estará mais disposto a trocar BTC por qualquer quantidade de *fiat*, como aconteceu em bolívares.

Distribuição de conhecimento e ondas de adoção e infraestrutura são recíprocas, formando um *loop* de *feedback* virtuoso e uma função de tempo e valor. À medida que o valor aumenta, o Bitcoin capta o interesse e a atenção de um público muito mais amplo de potenciais adotantes, que então começam a aprender sobre os fundamentos do Bitcoin.

Da mesma forma, uma base de ativos valorizada atrai capital adicional não apenas como uma reserva de riqueza, mas também para construir uma infraestrutura incremental (por exemplo, desenvolvimento tecnológico, mercado de compra e venda *Exchanges*, soluções de custódia, camadas de pagamentos, *hardware*, mineração etc).

No momento, o Bitcoin ainda é incipiente e a base de usuários provavelmente represente em torno de 1% a 2% do potencial global (em um mundo com 7,8 bilhões de habitantes e 70% adultos). Quando um bilhão de pessoas adotarem o Bitcoin, a noção da grandeza do seu valor decorrente do Efeito Rede será conhecida. Até lá, ciclos de alta volatilidade tendem a ocorrer (mesmo que decrescentes em termos reais e não em *fiat*) com os agentes aprendendo a precificar o ativo em um mercado cada vez maior, mais líquido e mais desenvolvido.

A volatilidade[396] do bitcoin em termos reais só diminuirá à medida que atingir a maturidade e a taxa de adoção se estabilizar – a redução da volatilidade no poder de compra se dará ao longo do tempo. Ou seja, se um bilhão de pessoas usarem bitcoin, os 100 milhões de adotantes subsequentes representarão apenas 10% adicionais da base. Tendo em vista que o fornecimento de bitcoin permanece com um cronograma fixo da sua oferta monetária, Charles Vollum, da *Pricedin Gold*[397], vem notando o declínio da volatilidade sobre a existência do bitcoin, novamente com o preço tanto em dólar como em ouro**:**

> Em 2011, o limite superior era cerca de 84x o limite inferior. Um ano depois, a proporção era de 47x. Em 2015, era 22x, e no início de 2020 havia caído para 12x. Isso é bom, demonstrando um declínio na volatilidade geral de pico ao vale. Se esse padrão persistir, a proporção será de cerca de 9x em meados de 2024 e cerca de 6,5x até o final da década. Ainda alto pelos padrões de *forex* e títulos, mas menos de 10% da volatilidade de 2011!

Enquanto a volatilidade em *fiat* é inevitável, sendo uma característica de qualquer ativo novo com características singulares (e não um *bug*), o influenciador *bitcoiner* e ex-engenheiro do *Google*, Vijay Boyapati, explicou no *podcast* de Stephan Livera[398] que "Os economistas do *establishment* ridicularizam o fato de que o bitcoin é volátil, como se você pudesse ir de algo que não existia para uma forma estável de dinheiro da noite para o dia; é completamente ridículo".

O que acontece entre as ondas de adoção é a função natural da descoberta de preços, à medida que o mercado converge para um novo equilíbrio, que nunca é estático. Nos ciclos de *hype* do Bitcoin, a ascensão, a queda, a estabilização e novamente a subida são quase rítmicas. Também são naturalmente explicadas pelo medo especulativo, seguido pelo acúmulo de conhecimento fundamental e pela adição de infraestrutura incremental. Roma não foi construída em um dia; no bitcoin, a volatilidade e a descoberta de preços são fundamentais para o processo.

Enquanto o Bitcoin vai adquirindo uma parcela na competição global por reserva de valor por conta de suas propriedades monetárias superiores, a função de uma economia é acumular capital que realmente torne nossas vidas melhores, não dinheiro. O dinheiro é meramente o bem econômico que permite que a coordenação acumule esse capital. Como o bitcoin é uma forma de dinheiro fundamentalmente superior, ele tende a ganhar poder de compra em relação aos ativos monetários inferiores (e substitutos monetários) e a ganhar cada vez mais participação de mercado na função de coordenação econômica, apesar de ser menos funcional como moeda transacional hoje.

O Bitcoin tende a se tornar moeda transacional ao longo do tempo. Nesse período de transição, seria muito mais lógico gastar um ativo depreciável (dólares, euro, iene, real, por exemplo) e economizar um ativo de valorização (bitcoin), seguindo o princípio monetário da Lei de

Gresham[399], que diz: “A má moeda tende a expulsar do mercado a boa moeda”. Num contexto destes, a Lei de Gresham prevê a ocorrência de um fenômeno de conservação por parte dos agentes da moeda “boa”, enquanto a moeda “má” é utilizada para efetuar os pagamentos (a exemplo do fenômeno do bimetalismo, em que a prata tinha mais velocidade de circulação como moeda de pagamento que o ouro, que passou a servir como reserva de valor).

Na trajetória do Bitcoin para a monetização completa, a reserva de valor deve vir como uma primeira ordem lógica, e o Bitcoin provou ser uma boa reserva de valor, apesar de sua volatilidade. À medida que a adoção amadurecer, a volatilidade relativa naturalmente cairá e *satoshis* se tornarão cada vez mais meio de troca direta. Como afirma Taleb: “Sistemas complexos que suprimiram artificialmente a volatilidade tendem a se tornar extremamente frágeis, enquanto ao mesmo tempo não exibem riscos visíveis.”

Em política monetária, as funções básicas de moeda são: 1º: reserva de valor, 2º: meio de troca e 3º: unidade de conta.

Se há uma bolha que deveria te preocupar, não deveria ser a bolha do bitcoin. “Bitcoin não é bolha, é a agulha que vai estourar a bolha das bolhas – a bolha do juro negativo, a bolha do consumismo, a bolha imobiliária, a bolha das ações, a bolha da previdência, a bolha dos títulos, a bolha do *welfare*; e a bolha do endividamento”.

Se o ativo permanecer seguindo seu padrão histórico, deve continuar tendo períodos de valorização exponencial seguidos de correções violentas, como já houve de até 90% (embora sejam menores as quedas posteriores), seguidas de períodos de acumulação (preço em lateralização).

Também é razoável considerar que, quanto maior for o seu valor de mercado e o seu grau de legitimação – como aconteceu com os mercados futuros da CBOE/CME em 2017 e aconteceu em 2020 com o início da negociação dos *ETFs* (*exchange-traded funds)* –, maior será a tendência de redução de volatilidade média com o tempo. Nassim Taleb, em seu livro *Skin in the game*, diz que “Coisas voláteis não são necessariamente arriscadas, e o inverso também é verdade”.

Em um cenário de hiperbitcoinização, haverá cinco classes de indivíduos:

a) Os Hugo Stinnes: alavancados maciçamente, na medida que a gestão de risco permite, serão premiados com aumento absurdo do patrimônio, como já ocorre com Saylor;
b) Os HODLers: experimentarão aumento absurdo do patrimônio, mas com muito menos risco;
c) Os *boomers* do *cash-and-carry:* receberão um prêmio de consolação (ex: rendimento de 100% numa moeda que perdeu 90% do poder de compra na hiperbitcoinização, ou seja, mitigarão a perda de 90 para 80%);
d) Os “diluídos”: verão o patrimônio alocado em ativos denominados em moeda *fiat* ou equivalentes (CDBs, dívida monetária, fundos de pensão etc) virar pó;
e) A turma da “carona”: que tem patrimônio não denominado em moeda (donos de imóveis e outros bens não-financeiros). Poderão ter leve aumento ou queda do patrimônio a depender de qual destes fatores será mais forte: a perda do prêmio monetário atribuído ao bem (imóveis, FIIs e ações); ou o ganho de prosperidade generalizado.

4) A demanda institucional: fase 4

> As empresas precisam do Bitcoin para proteger seus balanços. Enquanto os governos competem para desvalorizar suas moedas, muitas empresas não conseguem gerar um retorno positivo sobre o capital. Bitcoin protege a tesouraria.
>
> Brandon Quittem

A “fase 4”[400] do bitcoin ficou muito clara entre 2020 e 2021, com forte demanda institucional. Além do exemplo do GBTC da *Grayscale*[401] (viabilizando até recursos de *401k* e *IRA* serem alocados em bitcoins), empresas como *Microstrategy* de Michael Saylor, que virou grande entusiasta do Bitcoin; *Square* dirigida por Jack Dorsey grande defensor do Bitcoin, e diretor executivo do *Twitter*; *Tesla* comandada pelo polêmico Elon Musk; e até o Mercado Livre, uma das maiores empresa da América latina, e demais empresas[402] e gestoras de investimento adicionaram bitcoins a seus balanços.

Como mencionado, até mesmo a *BlackRock* (maior gestora de ativos do mundo) e outras gigantes estão começando a se expor ao Bitcoin, como *Citigroup*, *Paypal*, *Visa*, *Goldman Sachs*, *Morgan Stanley*, *Fidelity* e *JP Morgan*. Eventualmente, quem não a adicionar bitcoin às carteiras de clientes não vai ter como competir, caso os retornos históricos se mantenham.

Após fundos de BTC como o GBTC, a próxima etapa é o lançamento de *ETFs* (*Exchange-Traded Fund*, também conhecidos como fundos de índice, negociado em bolsa) de BTC – com menores taxas de administração e maior segurança para investidor de varejo e institucional. Essa foi a causa do encerramento das captações e o deságio sistemático do GBTC da *Grayscale*.

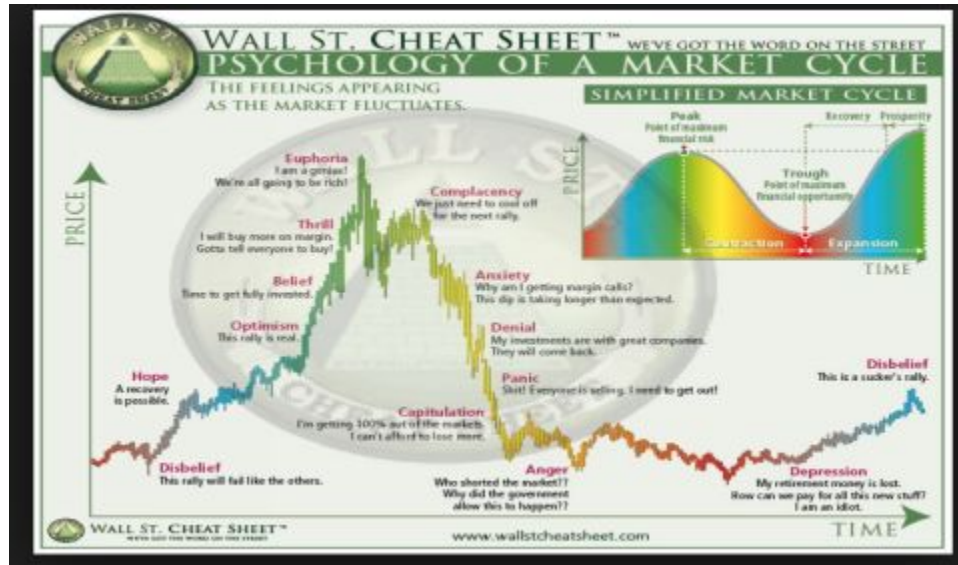
Dentre os *ETFs* e fundos com alguma exposição ao Bitcoin, podem ser citadas as brasileiras[403]: *Hash Dex* sob o código *HASH11* (fundo composto por bitcoin mais uma cesta de *altcoins* que mudam constantemente) e o produto da Q*R Asset Management*, da gestora de recursos da holding *QR Capital* sob o código *QTBC11* (100% bitcoin).

O Canadá também aprovou seu primeiro ETF de bitcoin da América do Norte e o primeiro do mundo, o *Purpose Bitcoin ETF* sob o código *BTCC* (acessível a cidadãos americanos e demais investidores, inclusive brasileiros, credenciados em *brokers* nos EUA, sob o código *BTCC.U-TO*).

5) Como analisar o mercado de bitcoin: FOMO e FUD

O bitcoin provou ser um ativo cíclico, com altas consideráveis de preços em períodos de *Bull Market* (mercado de alta). Em todos os estágios desses ciclos, há grupos de pessoas comprando, vendendo, fazendo *hodl*, negociando e minerando bitcoin. Para compreender totalmente a psicologia e as características desses ciclos de mercado, existem conjuntos de dados mais adequados para analisar além próprio livro-razão (*blockchain*) do Bitcoin. É possível explorar algumas métricas *on-chain* selecionadas que fornecem uma visão sobre sentimentos e os padrões de *hodlers*, especuladores e mineradores em sites como: *Skew, Coinmetrics e Glassnode*.

Há um ponto relevante a ser observado numa análise de mercado: *early adopters e smart money*, possuem um *modus operandi* semelhante (comprando em fundo e desovando em topos, como é evidente por análises *onchain*). Os compradores recentes de varejo que tendem a vender com perdas, as sardinhas.

O bitcoin tem um ciclo de, aproximadamente, 4 anos. Em cada um desses ciclos ou Eras, o preço passa a maior parte do tempo caindo (*bear barket*) e lateralizando. Nos 12 a 18 meses após o *halvening* há subida (*bull market*). O choque na oferta dos novos bitcoins (oferta marginal cai à metade) é o gatilho para aumento de preço que, quando passa dos padrões fundamentais, reverte para correção – igualmente exacerbada por ciclos emocionais[404]:

Se em 20 anos o fluxo líquido de dólares (seja nominal ou real) no ecossistema se mantiver, o bitcoin deverá custará 16x mais, *ceteris paribus* (considerando demais variáveis constantes). Para ficar claro: 16x mais a partir de US$50 mil seriam US$800 mil — ou seja, o BTC valer o equivalente a todo ouro no mundo.

Caso as moedas *fiats* morram, há o potencial de a riqueza nelas (US$ 100 trilhões) ser engolida pelo BTC e pelo ouro.

Voltando ao *halving*, toda vez que há redução da oferta marginal à metade, um novo processo de descoberta de preços (*bull run*) se inicial. A subida tem razão fundamental, mas qualquer ativo que sobe mais de 1.000% em um ano atrai gente que "comprou porque está subindo", causando o processo de excesso psicológico que o mercado chama de *FOMO* (*Fear of missing out*), ou "medo de ficar de fora".

Por isso, a cada ciclo, ocorre um momento de euforia que a cotação do bitcoin passa das métricas de análise técnica (como *Mayer multiple*)[405] e de análise fundamentalista (como *S2FX* e *S2F*)[406]. Quando a correção chega, as perdas são brutais, porque quem comprou pelo motivo de ter subido também vende porque está caindo. Neste caso há também um excesso psicológico que se chama *FUD (Fear*, *uncertainty and doubt)*, ou “medo, incerteza e dúvida”. Em resumo, o preço do Bitcoin é impulsionado por dois fatores principais, oferta e demanda: a) escassez exponencial, com uma curva de oferta assintótica tendente a zero; e, b) a adoção crescente, com o percentual de usuários de Bitcoin em 2020 sendo equivalente ao de usuários da internet em 1997.[407]

Há quem acredite que os ciclos de subida de dezenas de vezes seguidos de quedas de mais de 85% vão ser amenizados com o tempo: como os defensores da Hiperbitcoinização[408] (em decorrência da hiperinflação) e do “super ciclo”[409] (considerando que compradores institucionais seriam menos emocionais, amenizando subidas e quedas).

6) Quais os riscos do Bitcoin?

O Bitcoin compartilha dos mesmos riscos dos demais ativos financeiros: a) riscos legais: ser proibido, criminalizado, eventual prisão ou pena de morte para quem usar; b) risco operacional, parar de funcionar por *bug*, ataque bem-sucedido ou colapso societal (inverno atômico provocado por guerra atômica, meteoro, ou massa coronal destruir a rede elétrica ou Internet mundial); c) crédito: o bitcoin não tem, porque não é *IOU* (*I owe you* – É geralmente um documento informal que reconhece uma dívida), não é dívida como real, é ativo como ouro, mas as empresas do ecossistema têm esse risco, de ficar sem financiamento[410]; d) liquidez: não ter quem queira ou consiga comprar ou vender, sem *gateways* para tirar ou colocar moeda no sistema (por exemplo, consequência de congelamento de ativos em *exchanges* como Mike Maloney acha que vai acontecer no *reset* ou "Plano Collor Mundial"); e e) risco de mercado: preço cair em recessão mundial, como ocorreu em março de 2020 quando o bitcoin caiu mais de 50% em menos de uma semana.

A volatilidade do bitcoin, em grande medida, é reflexo da percepção de risco do ativo e da infância no seu desenvolvimento e no aprendizado em seus mecanismos de descoberta de preços. Alguns[411] argumentam que, em decorrência desses fatores, a tendência é que sua volatilidade seja reduzida; outros defendem que, no final das moedas fiduciárias, o valor do bitcoin subiria exponencialmente (como o valor de qualquer ativo onde há hiperinflação a ponto de a sociedade se desmonetizar, como na Alemanha de Weimar, Zimbábue ou Venezuela), cenário usualmente denominado como hiperbitcoinização.

7) O padrão Bitcoin: Por que o Bitcoin é o rei?

Efeito rede, Efeito Lindy e Proof of Brain

A maioria das criptomoedas são originadas do código base do Bitcoin, cujos protocolo e *software* são publicados abertamente; e, assim, qualquer desenvolvedor em todo o mundo pode acessar o código e modificá-lo ou copiá-lo, no todo ou em parte, fazendo sua própria versão modificada do *software* Bitcoin.

A rede Bitcoin compartilha um registro público na sua “cadeia de bloco” (*blockchain/timechain*), que armazena de forma imutável todas as transações, desde o seu lançamento em 2009, operando 24h por dia e 7 dias por semana.

O advento do Bitcoin é digno de total respeito, como grande conquista da ciência da computação na tecnologia – ao atingir escassez digital pela primeira vez na história. Em suma, o código do Bitcoin garante que apenas um número definido de novos bitcoins seja emitido, sem intervalos, a cada 10 minutos, em média, enquanto a experiência tiver sucesso e houver alguém rodando o *software*.

Como uma moeda pode ser distinguida da outra? E o mais importante, como um investidor pode saber qual será o valor em longo prazo de uma moeda?

A proposta real de valor do Bitcoin é resumida por Jimmy Song[412] (2019): “Quase todos os projetos de *altcoin*, *ICO* ou *hard forks* pregam que estão sendo inovadores de alguma maneira ao afirmarem superioridade ao Bitcoin em algum aspecto. Porém, esquecem que a maior inovação já aconteceu”. Por essa razão, maximalistas consideram essas modalidades (*ICOs* e *altcoins*) como espécies de fraude e estelionato.

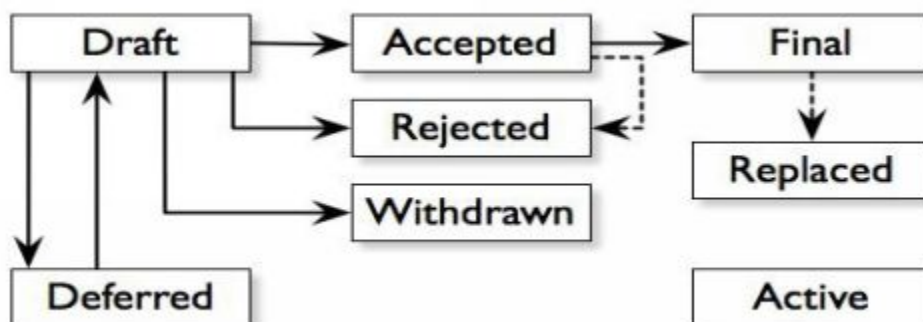
O Efeito Rede e o Efeito Lindy do Bitcoin são incomparáveis aos de outras criptomoedas, pois sua base de usuários (e por consequência maior capitalização de mercado), o número de *full nodes*, a capacidade de atrair melhores mentes em seu desenvolvimento *(Proof of Brain)*, seu ecossistema de negócios pujante com um mercado altamente inovador são muito maiores em qualquer métrica. Além disso, qualquer inovação ou melhoria das *altcoins* pode ser adotada no Bitcoin, como já aconteceu com a resolução do problema da maleabilidade e os *atomic swaps* entre *Litecoin* e *Decred*, por exemplo, que serviram de *testnets* para o Bitcoin com sucesso, mas desde então só tiveram seus valores em bitcoin em baixa para anos e anos. Como resume Vijay Boyapati[413]**:**

> Se o Bitcoin existir por 20 anos, haverá uma confiança quase universal de que estará disponível para sempre, da mesma forma que as pessoas acreditam que a Internet é uma característica permanente do mundo moderno.

A rede Bitcoin já possui um robusto *roadmap* de inovações – e muitas delas tendem a ser testadas antes em *altcoins* (além de sua *testnet*), demonstrando seus níveis de segurança e conservadorismo superiores.

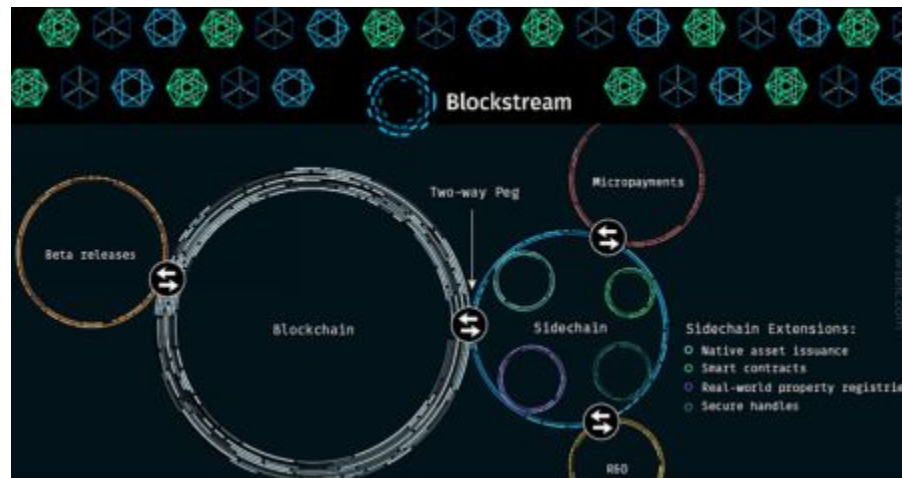
8) Roadmap e perspectivas: como escalar

Vários roteiros de desenvolvimento de inovações no Bitcoin já foram feitos desde 2015[414]. Essas metas não se cumprem integralmente – seja porque novas soluções superiores surgem ou por não haver implementação ou sequer desenvolvimento de propostas –, como se observa em diversas fontes jornalísticas, fóruns e relatórios financeiros[415].

BIP (Bitcoin Improvement Proposal) é uma maneira formal de transmitir sua ideia à comunidade de desenvolvimento. Os *BIPs* possuem um formato e modelos específicos e existe um editor *BIP* dedicado. Só porque um *BIP* é enviado não significa que ele será aprovado. Normalmente, este é o ciclo de vida do *BIP*[416]:

A autoria e o estado (rascunho, proposto, aceito, rejeitado…) de todos os BIPs (até agora do 1 ao 370) podem ser consultados publicamente[417], a maioria deles são incrementais e passam desapercebidos pelo usuário comum. Poucos são aqueles que mudam radicalmente tipos de endereços usados, funcionalidades ou custo de transação - como *SegWit* (BIP 141) e *Taproot* (BIP 343).

Os grandes focos dos BIPs recentes são: a) aumento de funcionalidades em *smart contract*s (facilitando *multsig*, *timelock* e soluções em outras camadas); b) redução de custo de transação e de tamanho das transações (aumento de eficiência); e, c) o aumento da fungibilidade, “monerização” do bitcoin.

Os grandes beneficiários desses BIPs são os projetos *Sidechain* (cadeias laterais) já operacionais, como as redes *RSK* e *Liquid***.** As cadeias laterais foram projetadas para permitir que outras *blockchains* se conectem à rede Bitcoin usando uma moeda separada que é referenciada ao bitcoin. Isto significa que cada *sidechain* é uma *blockchain* separada que pode ter regras diferentes da rede principal do Bitcoin enquanto ainda estiver conectada a ela. Isso permite que os usuários testem e desfrutem de novas funcionalidades de uma forma que não afete a *blockchain* principal, sem a necessidade de criar uma moeda digital.

Como ilustrado [418], são *sidechains* operacionais:

Liquid Network:[419] É uma *sidechain* privada, portanto, há algum controle sobre quem pode acessá-la. Os benefícios da *Liquid* são a permissão de transações instantâneas, a privacidade (transações confidenciais são incorporadas) e a capacidade de os usuários manterem fundos líquidos fora de uma *exchang*. Seu *token* é chamado de **LBTC** *(Liquid bitcoin*), sendo vinculado ao BTC na proporção de 1:1.

A rede se baseia no conceito "Cadeia Federada", que possui três partes principais no sistema: usuários; signatários de bloco, que são semelhantes aos mineradores; e vigias, que permitem que os fundos sejam transferidos para a cadeia de forma segura por meio de um processo conhecido como *pegging*. Foi desenvolvida pela empresa *Blockstream*.

***RSK (*Rootstock):**[420] É uma *sidechain* que planeja trazer funcionalidade de contrato inteligente e pagamentos quase instantâneos para a rede Bitcoin. Assim como a *Liquid*, ela usa um sistema federado, com os custodiantes rastreando o movimento do bitcoin entre a rede da *RSK* e a *mainnet* do Bitcoin. Ela faz isso usando um *token* chamado RBTC (Rootstock Bitcoin), que também é vinculado ao BTC na proporção de 1:1. Curiosamente, os contratos inteligentes no *RSK* são programados no *Solidity*, e a máquina virtual RSK é totalmente compatível com a da Ethereum. A rede da RSK é protegida por uma prova de trabalho, com o mesmo algoritmo do Bitcoin. Isso significa que as mineradoras de Bitcoin também podem dar segurança à rede *RSK* com muito pouco impacto no desempenho da mineração. A *RSK*

afirma ser capaz de escalonar para 100 transações por segundo usando verificação probabilística e provas de fraude, bem como *sharding*, algo que a Ethereum também está desenvolvendo. Anteriormente conhecida como *Rootstock*, a *RSK* é apoiada pela federação *RSK*, que é formada por mais de 30 empresas de *blockchain*, como *Xapo*, *Antpool*, *Bitpay e Digital Currency Group*. O CEO da *RSK* é Diego Gutierrez Zaldivar e foi lançada na rede Bitcoin em janeiro de 2018.

Dentre as melhorias recentes no Bitcoin, incluem-se:

***Segwit* (*Segregated Witness*)**: **Já implementado no protocolo do Bitcoin (via *soft fork*).** Foi proposta para além de mitigar um problema de limitação de tamanho de bloco na *blockchain*, que reduz a velocidade de transação do bitcoin (com isso demorando as confirmações na rede). O recurso também resolve o problema de maleabilidade das transações, dando espaço para a implementação de outras tecnologias de segunda camada, como a *Lightning Network*. Graças ao *SegWi*t e *batching*, as principais *exchanges* e *wallets* reduziram as taxas de transações na rede.

***Lightning Network*: Já possui aplicação prática[421].** Uma das propostas de solução em segunda camada para a rede do Bitcoin para dar escalabilidade, prometendo suportar um número quase ilimitado de transações fora da cadeia entre os usuários, e praticamente sem custos enquanto aproveita a segurança oferecida pela *Blockchain* do Bitcoin. Com "o futuro dos micropagamentos", os usuários poderão comprar o tão "sonhado cafezinho na padaria" pagando frações ou quase nenhuma taxa de transação. Empresas como *Lightning Labs*, *Blockstream*, ACINQ e ZAP *Lighting* desenvolvem aplicações para a rede LN[422]:

Innovations in Bitcoin
Layer 2
Sidechains
Performance & Usability
Mining
Smart Contracts
Privacy
Channel Factories
eltoo
Atomic Swaps
Private Messages
Omni DEX
Microsoft ION
Open Timestamps
VeriBlock
Issued Assets
Lightning Network
Omni
Identity
Data Anchors
Rootstock
Drivechain
Elements
Liquid
MuSig
Cross-Input Aggregation
Schnorr Signatures
Neutrino
Erlay
BTCPay
uTreeXo, libMiniSketch, Tx Accumulators
FIBRE
BetterHash
Stratum
Stratum V2
Mining Derivatives
CheckTemplateVerify
tBTC
MAST/ Taproot
Scriptless Scripts
Simplicity
Ivy
Hivemind
CoinJoin
Dandelion
Confidential Transactions
CoinSwap
G'root
Tapscript
ZeroLink
P2EP
SNICKER
Value Shuffle
Bulletproofs
TumbleBit

> Bitcoin é o projeto mais ambicioso que a humanidade está construindo hoje - garantir os direitos de propriedade e o futuro financeiro de 7,8 bilhões de pessoas com nada além de um simples smartphone. @DocumentingBTC[423]

***Schnorr Signatures/Taproot*:** Agregam várias assinaturas de transações em uma única assinatura. Isso reduz um pouco o tamanho da transação (redução no tempo de confirmação das transações) e inibe chances de futuros ataques de *spam* na rede Bitcoin.

> A assinatura Schnorr é considerada o mais simples esquema de assinatura digital para ser comprovadamente segura em um modelo *de oráculo* aleatório. [2] É eficiente e gera assinaturas curtas. Ela foi coberta pela patente US 4.995.082, que expirou em fevereiro de 2008. Wikipédia[424]

As assinaturas de Schnorr trazem uma enorme melhoria em fungibilidade, privacidade, escalabilidade e funcionalidade. Finalmente, a implementação de assinaturas de *Schnorr* poderia permitir desenvolvimentos futuros para o Bitcoin, como contratos inteligentes.

O *Taproot*[425] permite pagamentos ao *hash* da chave pública, que pode opcionalmente ser passada para um *script*.

Moedas protegidas pela *Taproot* podem ser emitidas, seja cumprindo o *script*, seja fornecendo uma assinatura que é verificada contra a chave pública. O *Taproot* destina-se a ser utilizado com assinaturas Schnorr, o que simplifica a criação de *scripts* multipartidários (por exemplo, com *MultiSig*). O *soft fork* também deve permitir que a *Lightning Network* mude de HTLCs para *Payment Points*, o que também é uma grande melhoria para a *Lightning Network* em termos de privacidade.

Das implementações futuras, podem ser enumeradas:

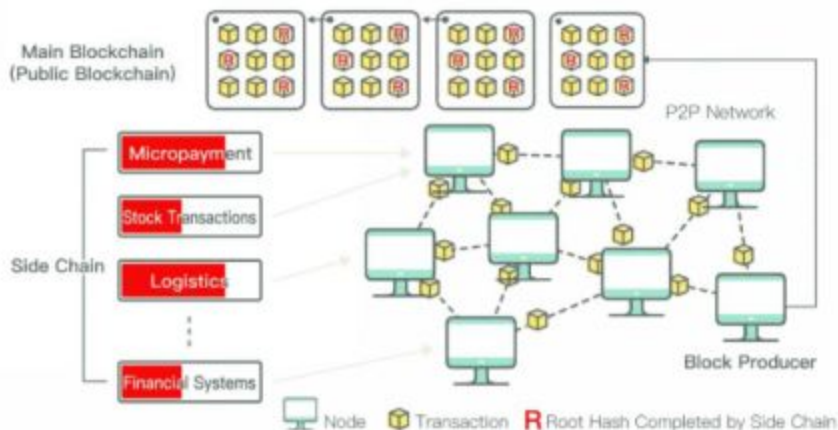
***Bulletproofs*: Ainda sem data definida, estando na fase de discussão e pesquisa entre desenvolvedores**. A tecnologia oculta quantidades de transações entre o remetente e o receptor para maior privacidade com o mínimo de poder computacional necessário para processar uma transação. Desenvolvido por Jonathan Bootle, da University College of London, e Benedikt Bünz, de Stanford, o *bulletproofs* é prova de conhecimento zero, o que significa que não se exige qualquer confiança entre as partes.

O *Bulletproofs* atraiu a atenção de outras criptomoedas, como Monero, que já implementou em seu protocolo, e Litecoin, que considera implementar. A tecnologia também é leve e não aumenta maciçamente a quantidade de energia computacional necessária para processar transações, podendo funcionar bem em *blockchain*s públicos como o Bitcoin.

***Confidential transactions* (CT): Ainda sem data definida, está na fase de discussão e pesquisa entre desenvolvedores**. As transações confidenciais (*TC*) manteriam as quantias de transações de bitcoins visíveis apenas entre os participantes da operação. A *CT* foi discutida por Adam Back, cofundador e *CEO* da *Blockstream*, em um fórum de discussão em 2013, sendo esse trabalho realizado pelo desenvolvedor Greg Maxwell. Em novembro de 2017, Maxwell anunciou que reduziu de 16 vezes o tamanho das transações (*CT*) normais de Bitcoin para apenas três vezes.

Drivechain: Ainda sem data definida, estando na fase de discussão e pesquisa entre desenvolvedores. O *Drivechain* planeja permitir que várias *blockchains* sejam vinculadas à *mainnet* do Bitcoin. Assim como a *RSK*, as cadeias laterais de *Drivechain* construídas podem ser protegidas por mineradores de Bitcoin usando mineração mesclada. Ao contrário da *RSK*, a

Drivechain é flexível e os desenvolvedores podem criar cadeias laterais *(sidechains)* adaptadas às especificações desejadas, como tamanhos de bloco maiores ou recursos de privacidade.

Essa implementação exigiria uma atualização no nível do protocolo, ou *soft fork*, e separa as alterações necessárias em duas partes: depósito de *hashrate* e mineração cega fundida. O *Drivechain* foi inventado por Paul Sztorc (que também criou o *Hivemind*), com a ajuda de Chris Stewart, Jason Dreyzehner, do *BitPay* e do desenvolvedor pseudônimo *Cryptaxe*.

***MAST*: Incorporada na atualização do pacote Taproot**.[426] *MAST é a* abreviação de *Merkelized Abstract Syntax Trees*, propõe melhorar o Bitcoin alterando a forma como os contratos inteligentes são gravados na *blockchain*. Com efeito, permite que os contratos inteligentes sejam divididos em suas partes individuais.

O *MAST* aumenta a privacidade mantendo partes ocultas e não utilizadas de contratos inteligentes, vinculando menos informações às chaves públicas. Também pode reduzir o tamanho da transação, uma vez que somente as partes preenchidas de um contrato inteligente são gravadas na *blockchain*. Finalmente, tem o benefício de permitir contratos inteligentes maiores. Bitcoin tem limites de tamanho de *byte* em *scripts*, o que limita seu tamanho geral. Mas, se um contrato inteligente pode ser quebrado em pedaços e escrito na *blockchain* em várias transações, então ele pode ser maior.

***Mimblewimble*: Ainda sem data definida, estando na fase de discussão e pesquisa entre desenvolvedores**. Oferece privacidade por padrão, mais fungibilidade[427] e melhor capacidade de escala da rede.

Como não oferece suporte a *scripts*, ele provavelmente seria implementado como uma *sidechain*.

8.1) Camada base (*onchain*), 2º camada e *sidechain* (cadeia laterais):

Numa rede monetária, é inevitável o "Trilema da Escalabilidade"[428]: segurança, descentralização e velocidade.

É impossível maximizar todos os três ao mesmo tempo numa só camada. Por *design*, foram priorizadas a segurança e a descentralização na camada base do Bitcoin.

Para viabilizar os três atributos, a rede precisa que outros protocolos sejam construídos em cima do protocolo base principal (seguro e descentralizado). Assim, os três atributos podem ser alcançados por meio de camadas superiores (2ª camada e *sidechains*), na qual cada uma irá priorizar atributos específicos. Como Hal Finney já expressava desde 2010.[429]

Como Nick Szabo[430] já expressava em 2017, registros *onchain* são a camada mais segura, como o *swift* para o sistema bancário, que possibilita as demais transações menos criticas serem liquidadas internamente. A camada base (*layer* 1) precisa ser a mais sólida e segura possível, sua falha seria a morte do sistema. Para a camada 2 e *sidechains*, pode haver menos segurança e mais velocidade e flexibilidade.

Operar *onchain* em alguns anos vai ser tão comum quanto transferir bens em cartório ou fazer remessas via *Swift*. *Sidechains* e 2ª camada, como a rede *liquid network* e *lightning network*, permitem transações ilimitadas em fração de segundo por centavos ou grátis, são seguras e permitem a privacidade nas transações.

O Bitcoin é a camada base para tokens mais eficientes em seus respectivos nichos: a) há mais de 2.300 BTCs aportados (Capacidade de rede)[431] na *Lighting Network*, que consomem milhões de vezes menos transações do que uma operação de cartão de crédito; b) há mais de 3.200 LBTC na *Liquid Network*, com *fee* fixa (equivalente a 1 satoshi/vbyte), blocos a cada 1 minuto e *confidential transacionas;* e, há mais de 2.020 RBTC na *RSK*[432].

Outros exemplos de protocolos construídos em cima da rede principal do Bitcoin, soluções de 2ª camada e *sidechains*, sejam elas já construídas ou em andamento são: a) *drivechains*[433]; b) *statechains* [434]; e, c) contratos inteligentes RGB[435]; d) Impervious[436]; e) *Stacks*[437].

Produtos já operantes em 2ª camada / *Sidechains* / *Discreet log contracts (DLCs)*:

- *SovrynBTC*
- *RSKsmart*
- *RIF Network*
- *Rsk Swap*
- *Moneyonchaino*
- *Wallets lightning network*
- Plataforma de Derivativos LNM e Kollider
- *Wallet RGB* (em construção)
- *Atomic Finance*
- *Suredbits*
- Dentre outros...

9) Stock to Flow (S2F) & S2FX – bitcoin valuations

“Todos os modelos são falhos, mas alguns são úteis."
George Box

O modelo *Stock-to-Flow* do Bitcoin foi construído pelo misterioso investidor institucional cuja personalidade no *Twitter* é conhecida apenas como *PlanB*[438], com artigos publicados em seu *blog* no *Medium*[439] (/*@100trillionUSD*), onde o leitor pode pesquisar e entender mais sobre a proposta de modelo para precificar o Bitcoin.

Este modelo trata o Bitcoin como comparável a *commodities* como ouro, prata ou platina. São conhecidas como mercadorias de “reserva de valor”, porque retêm valor por longos períodos devido à sua relativa escassez.

O *Stock to Flow (S2F)* mostra quantos anos são necessários para a taxa de produção atual atingir o estoque (reservas existentes), portanto, uma relação consistente entre razão de estoque e fluxo e o respectivo preço (medido pelo *market cap* total do ativo).

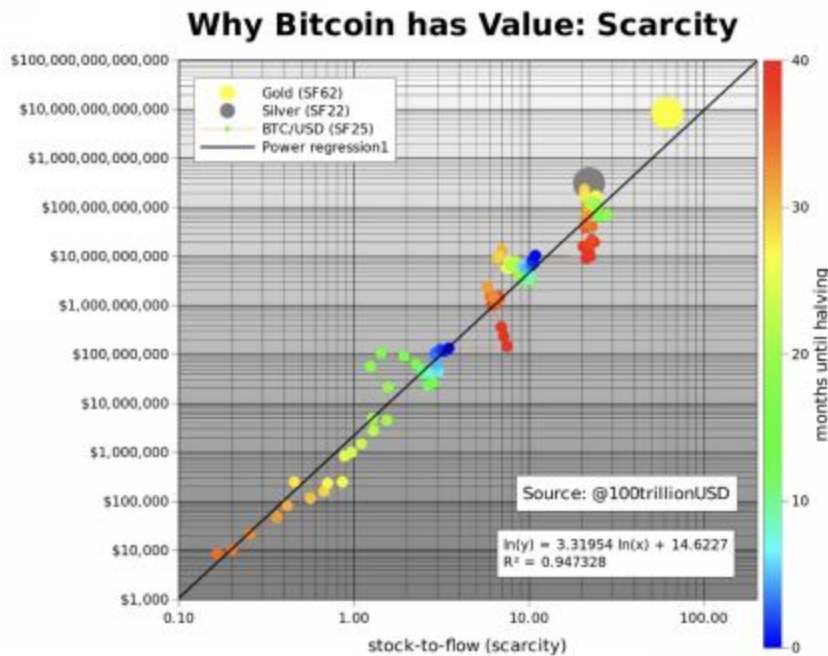
Aplicando ao bitcoin, como sua razão de escassez é crescente e predeterminada, métodos de avaliação com valores exponencialmente maiores foram desenvolvidos, aplicando as correlações identificadas em outros ativos.

A definição de escassez no dicionário remete a de algo difícil de ser encontrado na natureza ou reproduzido em laboratório; muito similar aos metais preciosos. Quando algo se torna escasso o suficiente, pode ser usado como dinheiro. A relação entre estoque e fluxo (*S2F*) é definida como a divisão entre a produção anual e o estoque atual.

***SF* = estoque / fluxo**

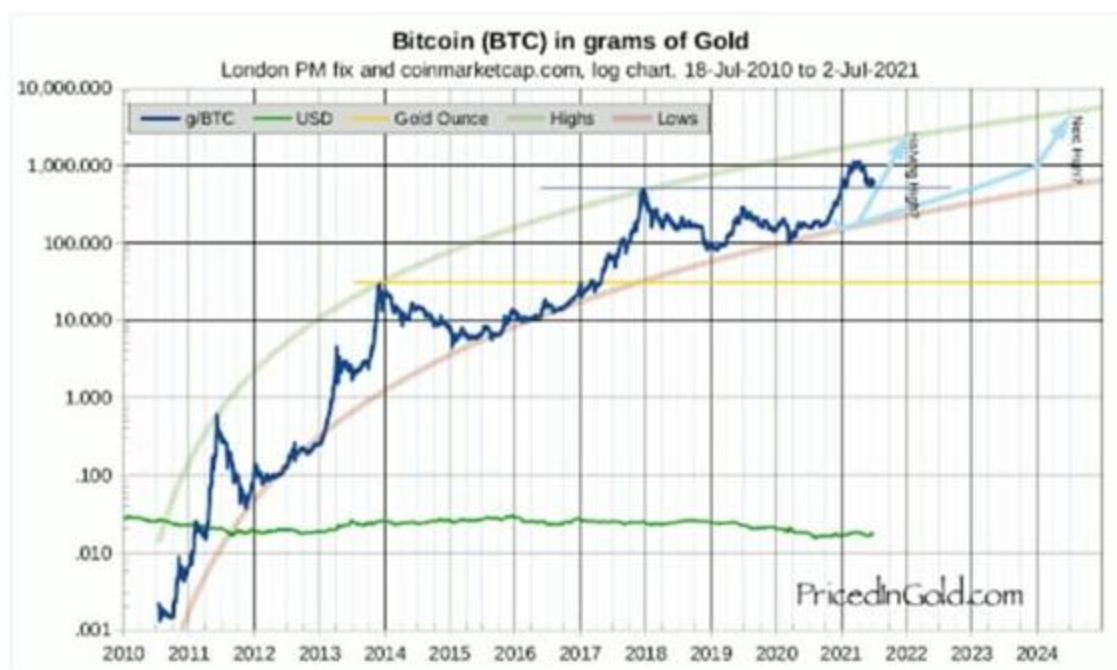
O uso do modelo bitcoin *S2F* não é realmente para negociação, mas para operações táticas de alocação de ativos.

Após a demonstração formal de que o modelo do *S2F* não tinha valor preditivo[440] e que, dentre outros problemas, o *S2F* deriva do preço e não o oposto (relação de correlação e não causalidade), o autor tentou contornar o problema com o *S2FX – Stock to Flow Cross Asset Model* (usando relações

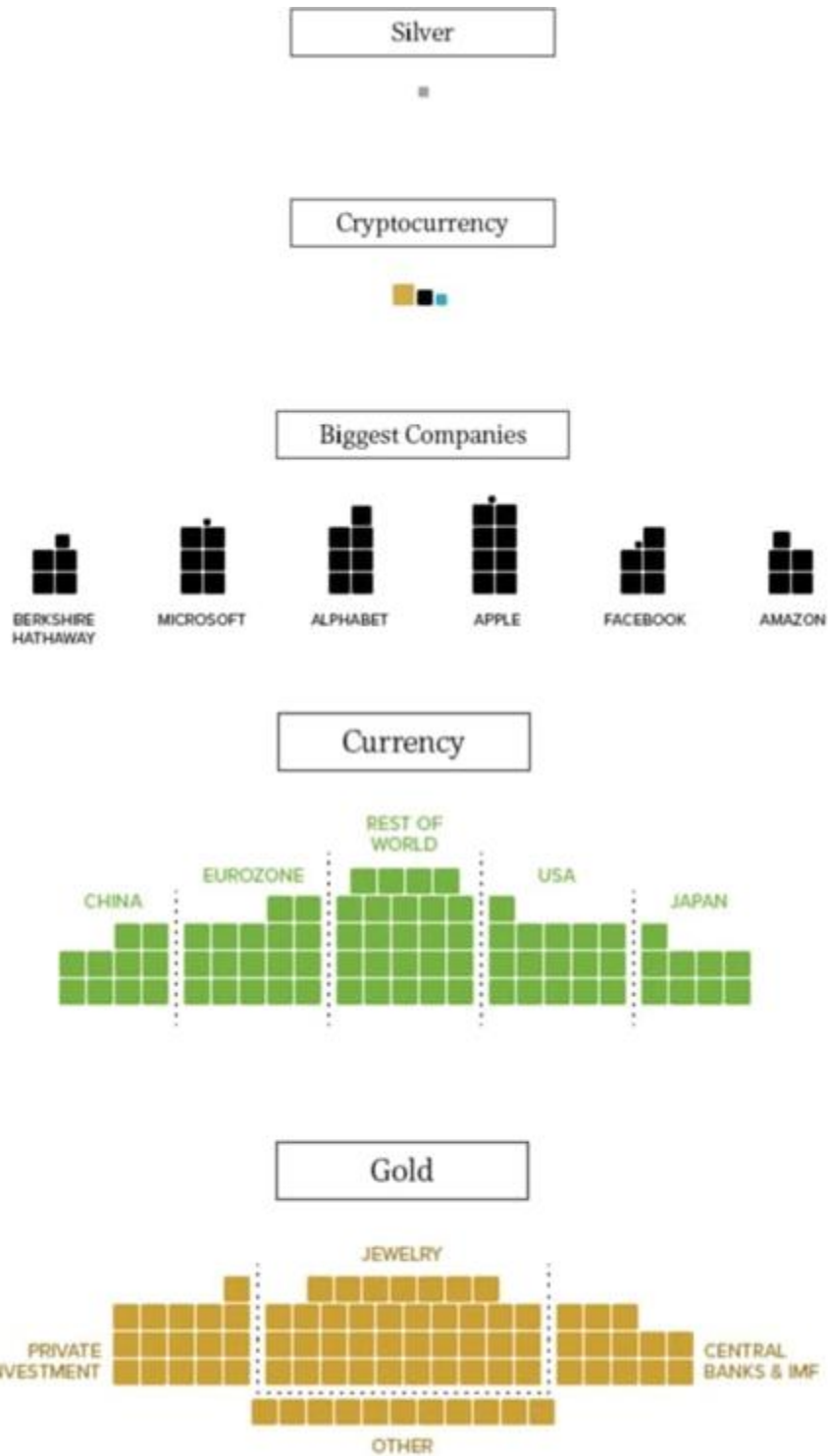
entre ativos, sem variável de tempo).

Existem dezenas de modelos preditivos como o *FF*, *bitcoin rainbow chart*, *Bitcoin VWAP price*, *CVDD* e outros[441] – usualmente apresentando padrões exponenciais.

Outro modelo com grandes evidências lógicas e empíricas é o *valuation* pelo custo mínimo de mineração[442]. O racional é que mineradores[443], em regra, não operariam no prejuízo e o valor mínimo de mineração seria um valor “piso" para a cotação do bitcoin – embora a autocorrelação entre preço e cotação possa tornar essa causalidade espúria[444]:

Bitcoin's Cost of Production
$1,00,000.00
$10,000.00
$1,000.00
$100.00
$10.00
$1.00
Price
29-03-2011
29-09-2012
29-03-2014
29-09-2015
29-03-2017
29-09-2018
Date
Cost of Mining 1 BTC (CapEx + OpEx)
Actual Price

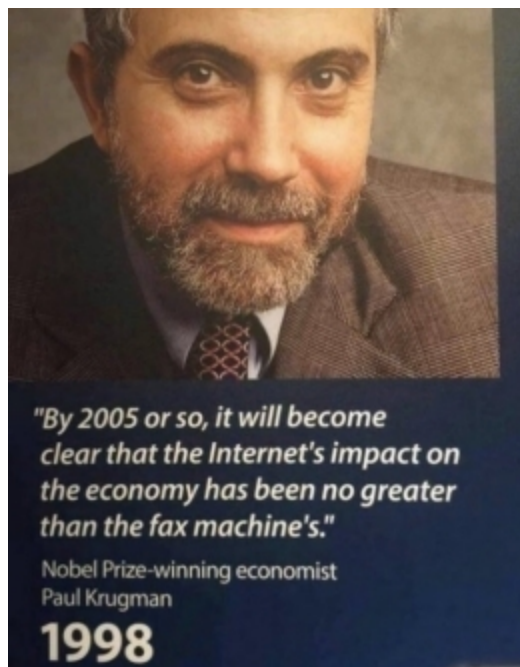
Charles Vollum, da *PricedindGold.com*, sugere em um artigo[445] um aumento de mais de 10x nos próximos anos (se voltar ao topo da faixa histórica), o que implicaria um preço em dólar de seis dígitos (como o modelo do *PlanB*), se o ouro permanecer relativamente estático em termos de dólar. No entanto, ele também observa que historicamente tem sido menos explosivo em cada ciclo (em gramas de ouro):

Minha análise começa observando as alturas e os tempos relativos das elevações em meados de 2011, final de 2013 e final de 2017. O segundo pico é cerca de 48 vezes maior que o primeiro, enquanto o terceiro pico é de cerca de 17x o segundo. Portanto, a taxa de crescimento nos picos parece estar diminuindo.

Chales Vollum

Irrelevância do Bitcoin nos mercados[446]

10) Ameaças ao Bitcoin

Existe um rol de centenas de pessoas que já decretaram a morte do bitcoin, desde ganhadores de prêmio Nobel, *CEOs* de grandes corporações e

líderes políticos mundiais. Todos erraram e, até agora, viraram alvo de risos e piadas. A lista de obituários do bitcoin (*bitcoin-obituaries*)[447] conta com inúmeros registros de "decretação" da morte do Bitcoin em mídias de grande circulação.

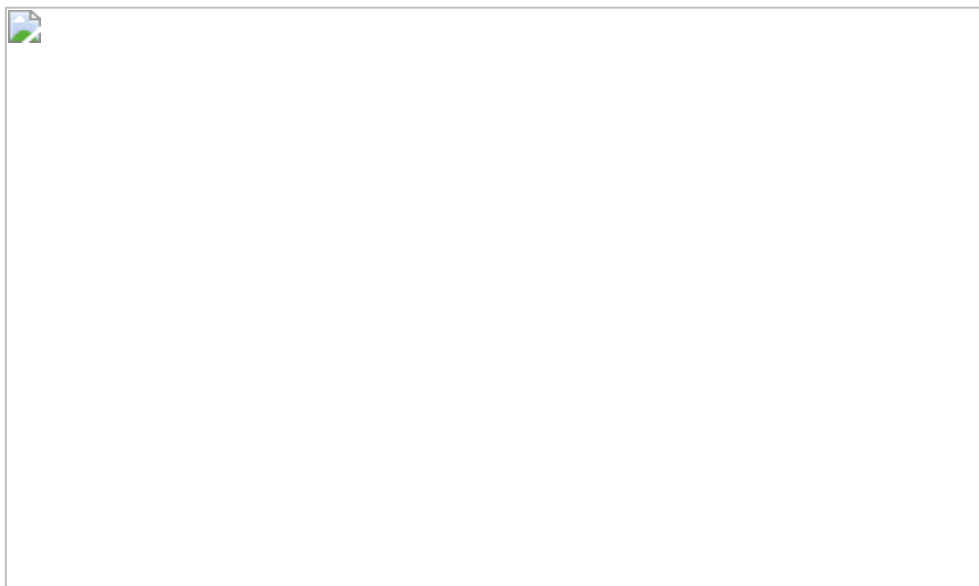
O destaque nessa categoria de "vergonha alheia", ou como prefere Taleb "*intelectual yet idiot*", é Paul Krugman – que, em 1998, também disse que a Internet não iria mudar a economia mais do que o aparelho de fax.

O Bitcoin pode ser destruído caso a rede mundial de computadores seja comprometida, assim como também será comprometido o resto da economia mundial.

Se a criptografia do Bitcoin for comprometida por computação quântica[448], as dos governos e bancos também serão (e com valores bem mais significativos).

Se o fornecimento global de energia elétrica for comprometido, a última preocupação de um ser humano será o Bitcoin – já que voltaríamos em semanas aos níveis tecnológicos e à capacidade de suporte do século XVII, com a maioria das pessoas no mundo mortas de fome ou em decorrência do caos.

Como todo ativo financeiro, o bitcoin está exposto a riscos operacionais (como *bugs*), legais (ser criminalizado) e de mercado (fortes variações de cotação). Como o bitcoin é um *token* de uso – e não de *equity* nem de dívida –, não carrega risco de liquidez nem de crédito, embora contratos (como empréstimos colateralizados) e empresas do ecossistema apresentem esses riscos, visto que nesses casos as chaves-privadas estão na posse de terceiros.

Se o Bitcoin não tivesse riscos inerentes, não teria o potencial de ganho sistemático já comprovado. O bitcoin é um *hedge*, um seguro, contra o sistema convencional por não apresentar correlação relevante com os ativos tradicionais e tender a performar melhor quanto piores forem as decisões de governos. Também por isso já se defende que é uma nova categoria de ativo.

A taxa de adoção de novas tecnologias usualmente segue curva em U invertido: primeiro com adoção exponencial de criadores pioneiros, *early adopters*, *smart money*; e, só por fim, da maioria das pessoas, como ilustrado na *Roger's Bell Curve*[449]:

As figuras anteriores demonstram como em 2020 o valor de mercado do Bitcoin ainda é irrelevante, se comparado a outros mercados e até a algumas empresas. Não há como prever se sua evolução exponencial vai encontrar um platô em termos reais (curva S da maioria das tecnologias) ou se vai continuar aumentando em termos nominais em *fiat*, como previsto na hiperbitcoinização (curva em J).

Não há como prever se o Bitcoin vai morrer ou se será o início da conversão de praticamente todos os ativos para as nuvens. O que se pode afirmar com certeza é que o Bitcoin resolveu demandas que existiam desde o milênio passado (dinheiro digital descentralizado de Friedman e moeda privada imune à jurisdição de Hayek) com a solução do problema de confiança mútua dos generais bizantinos, e sua tecnologia não será facilmente esquecida. Agora a humanidade não vai depender mais da confiança de terceiros para ter acesso à reserva de valor transmissível por qualquer meio de comunicação, mantida e autenticada sem qualquer custo de corretagem ou administração.

Bem-vindo à Era Digital, parabéns por descobrir o Bitcoin antes da maioria das pessoas. Nos próximos anos, ficará claro quem vai ganhar a corrida tecnológica: se os governos e grandes corporações, cada vez mais totalitários e corruptos, ou os indivíduos. Só depende das nossas decisões no presente – se uma qualidade suficiente de produtores se recusar a financiar os parasitas, ficará claro que Satoshi Nakamoto é John Galt, provocando o colapso dos Estados Sociais.

Ou o Bitcoin tirará dos governos o poder de criar moeda, de se endividar e de controlar taxas de juros, propiciando um renascimento moral, tecnológico e material, com mudanças brutais das preferências temporais derivadas do acesso a boas reservas de valor; ou a humanidade experimentará decadência moral, tecnológica e material, em um período de totalitarismo sem precedentes, com governos recebendo informações de grandes corporações e usando gamificação para motivar competição agressiva de obediência e eliminação de dissidentes.

Você pode levar um ser humano à autossoberania, mas não pode fazê-lo suportar o ônus da responsabilidade pessoal.
Jameson Lopp

Se você não acredita em mim ou não entende, eu não tenho tempo para tentar te convencer, desculpe-me… (HFSP)
Satoshi Nakamoto

DICAS COMPLEMENTARES

Livros:

- *The Bitcoin Standard* (Saifedean Ammous)
- *The Fiat Standard* (Saifedean Ammous)
- Bitcoin – A moeda na era digital (Fernando Ulrich)
- *The Ethics of Money Production (Jörg Guido Hülsmann)*
- *The Price of Tomorrow: Why Deflation is the Key to an Abundant Future* (Jeff Booth)
- O que o Governo Fez com o Nosso Dinheiro (Murray Rothbard)
- *Mastering Bitcoin (*Andreas Antonopoulos*)*
- *Grokking Bitcoin (Kalle Rosenbaum)*
- Bitcoin - A Internet do Dinheiro (*Andreas Antonopoulos)*
- *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money (Nathaniel Popper)*
- *Bitcoin Billionaires: A True Story of Genius, Betrayal and Redemption (Ben Mezrich)*
- *Bitcoin Money: A Tale of Bitville Discovering Good Money (Michael Caras)*
- *From Bitcoin to Burning Man and Beyond (John H. Clippinger)*
- *Trilema*: www.trilema.com/category/bitcoin/ *(*Mircea Popescu*)*
- *The Little Bitcoin Book* (Luis Buenaventura e Jimmy Song*)*
- *Thank God for Bitcoin (*Jimmy Song, Gabe Higgins e outros*)*
- *The Blocksize War (*Jonathan Bier*)*
- *The Bullish Case for Bitcoin (*Vijay Boyapati*)*
- *Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies (*Nik Bhatia*)*

Filmes e Séries:

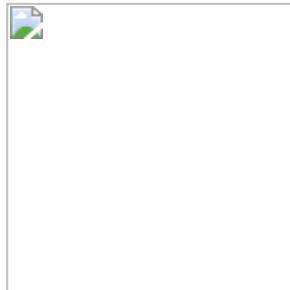
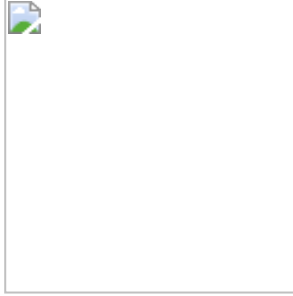
- Bitcoin: O Fim do Dinheiro como Conhecemos (*Bitchute*)
- *The Bitcoin Gospel (YouTube)*
- *Hidden Secrets of Money (YouTube)*
- *Banking on Bitcoin (Netflix)*
- *The Rise and Rise of Bitcoin (Vimeo)*
- *Ulterior States (YouTube)*
- *The Internet´s own Boy (HBO)*
- *TPB AFK (YouTube)*
- *Hard Money Film (Vimeo)*

POSFÁCIO

Se gostou do conteúdo, envie um *e-mail* (bitcoinblackpill@protonmail.com) ou ingresse no grupo do *Telegram* (Bitcoinblackpill_BR) para receber as publicações subsequentes.

Para referências completas e imagens coloridas e com alta definição,
Acesse nosso site: www.bitcoinblackpill.com

Gostaria de reconhecer o nosso trabalho de alguma forma?

Financie continuidade do projeto:

Doe Bitcoin pela Lightning Network

Endereço bitcoin:
bc1qptfh5hrnyasty7l2c3xta5cpvsrralm98z7243

ANEXOS

ANEXO I: Cartilha do MPF sobre criptos: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/cartilhas/atuacao-interinstitucional-com-o-bb/cartilha-moeda-digital-versaoatual.pdf.

ANEXO II: Criptomoedas, orientações gerais para equipes de buscas (Polícia Federal do Brasil): https://www.criptofacil.com/wp-content/uploads/2019/04/1_5046474950894944324-2.pdf.

ANEXO III: *3 Reasons I'm Investing in Bitcoin*: https://www.lynalden.com/invest-in-bitcoin/ - (arquivado: https://archive.vn/TXeuS).

ANEXO IV: Paul Tudor Jones: *The Most Compelling Case For Owning Bitcoin:* https://seekingalpha.com/article/4345426-paul-tudor-jones-compelling-case-for-owning-bitcoin - (arquivado: https://archive.vn/EcKsL).

ANEXO V: Parker Lewis: *Gradually, then Suddenly:* https://drive.google.com/file/d/1hcWezZLPV5MUQ_btezCv6p_H5g9loSUF/view - (arquivado: https://archive.vn/EMq8n).

ANEXO VI: *Bitcoin Investment Cases of Fidelity, Grayscale, VanEck, MicroStrategy:* https://github.com/100trillionUSD/bitcoin/find/master.

APÊNDICE: Resumo Tributário

Não é possível regular ou controlar diretamente o uso privado dos criptoativos, pois os *tokens* podem ser transferidos para qualquer país em minutos via Internet, por telefone, satélite, rádio ou até por memorização da *seed phrase*. A regulação estatal atua sobre as instituições formais submetidas à soberania estatal – corretoras, *gateways*, *P2P*, serviços de custódia ou contribuintes, pessoas naturais, que prestem voluntariamente as suas informações.

Abaixo seguem as normas regulatórias da Receita Federal:

Tributos - pagamentos - SRF/IN 84 de 2001

IR – ganhos de capital em outros direitos:
Isento até R$ 35.000 por mês;
de 35 mil até 5 Milhões, 15%;
de 5 a 10MM, 17.5%;
de 10 a 30MM, 20%;
Acima de 30MM, 22,5%

Procedimento atual: declara pelo GCAP, gera DARF e paga até o mês posterior.

INSTRUÇÃO NORMATIVA Nº 1.888 DE 2019
Tributos - compliance – Receita Federal do Brasil

GLOSSÁRIO

1. Altcoin: Criptomoeda alternativa, criada após o Bitcoin.

2. Ataque de 51%: Um ataque de 51% pode ser executado contra rede blockchain que utiliza o algoritmo de consenso PoW, no qual uma única entidade ou organização consegue controlar a maioria do hashrate, podendo causar e explorar falhas no sistema. O atacante teria os seguintes poderes: poder de mineração suficiente para excluir ou modificar a ordem das transações de forma intencional; fazer retroceder transações, o que poderia acarretar um problema de double-spending (gasto duplo); o fraudador pode impedir que algumas ou todas as transações sejam confirmadas (processo conhecido como ataque de negação de serviço) ou impedir que alguns ou todos os mineradores continuem seu trabalho, monopolizando mineração. O atacante não pode: reverter transações de outros usuários ou impedir que novas transações sejam criadas e transmitidas à rede; criar moedas do nada; mudar a recompensa dos blocos; ou roubar moedas que nunca lhe pertenceram.

3. AT (Análise técnica): Análise Técnica é uma ferramenta utilizada tanto por especuladores profissionais, como por amadores para análise do movimento de preço de alguns ativos financeiros, com base na oferta e procura destes.

4. *AML* (*Anti Money Laundering* – Antilavagem de Dinheiro): É um termo que se refere às regulamentações impostas em uma indústria financeira, em um esforço para prevenir e deter atividades ilegais. A lavagem de dinheiro indica ocultar a origem dos fundos. Diferentes jurisdições usam diferentes leis de *AML* para garantir que dinheiro “sujo” não seja recolocado no sistema.

5. Alavancagem (*leverage*): É uma estratégia de investimento que usa dinheiro emprestado – especificamente, o uso de vários instrumentos financeiros ou capital emprestado – para aumentar o potencial retorno de um investimento.

6. Algoritmos: Um algoritmo é uma sequência finita de ações executáveis que visam obter uma solução para um determinado tipo de problema.

7. Arbitragem (*arbitrage*): É a compra e venda de um ativo para lucrar com uma diferença no preço entre mercados. É uma operação que lucra

explorando as diferenças de preço de instrumentos financeiros idênticos ou similares em diferentes mercados ou de diferentes formas. A arbitragem existe como resultado de ineficiências do mercado e, portanto, não existiria se todos os mercados fossem perfeitamente eficientes.

8. Antifrágeis: Coisas que se beneficiam com o caos. A antifragilidade, um neologismo proposto por Taleb, seria o exato oposto da fragilidade, estando além da resiliência ou da robustez. O resiliente resiste a choques e ao tempo e permanece o mesmo, o antifrágil fica melhor. Esta propriedade estaria por trás de muitas coisas que mudaram com o tempo: desde ideias até mesmo a própria existência do ser humano como espécie.

9. ASIC**:** Acrônimo de "*Application Specific Integrated Circuit*" (Circuito Integrado de Aplicação Específica), é um *chip* criado especificamente para realizar uma tarefa. No caso do Bitcoin, os *ASICs* foram criados para processar hash SHA-256 e minerar blocos com maior eficiência.

10. Ancapistão: É uma sociedade em que não existe a figura do Estado e os indivíduos podem escolher a qual tipo de governança desejam se submeter. O respeito à propriedade privada e ao livre mercado é a prioridade; serviços como educação, saúde, segurança (pública e privada), tribunais seriam fornecidos por concorrentes privados em vez de coercitivamente pelo Estado.

11. *Bail-in* (Resgate interno): Quando o dinheiro do depositante (sócio ou credor) é usado para tratar a má saúde financeira dos bancos. Por exemplo, quando a Bitfinex hackeada alegava não ter bitcoins para quitar todos os saldos na plataforma e descontou valores dos saldos sacados até a sua recuperação.

12. *Bail-out* (Resgate externo): Quando o recurso externo normalmente “dinheiro público”, é usado para tratar a precária saúde financeira de uma instituição financeira à beira da falência. O governo simplesmente dá dinheiro (na forma de empréstimos, títulos e até em dinheiro) ao banco enfermo para sua sobrevivência.

13. *Backwardation*: ocorre quando o preço futuro é menor do que o preço à vista (*spot*), quando é possível fazer renda fixa em BTC vendendo presente e comprando o futuro. Situação oposta ao ***contango***, em que o valor futuro é maior que o *spot* e é possível fazer *cash and carry,* consolidando renda fixa em dólar.

14. *Betting* (Aposta): É a ação de apostar dinheiro, bens, tempo ou qualquer outra coisa no resultado de algo, como um jogo ou corrida. Em

outras palavras, o ato ou prática de jogar jogos de azar para uma aposta; geralmente em dinheiro.

15. Bit: É uma unidade comum para designar uma subunidade de bitcoin – 1.000.000 de bits é igual a 1 bitcoin. Esta unidade é geralmente mais conveniente para colocar preços em gorjetas, produtos e serviços.

16. Bimetalismo: É o termo econômico para um padrão monetário em que o valor da unidade monetária é definido como equivalente a determinadas quantidades de dois metais, tipicamente ouro e prata, criando uma taxa fixa de troca entre eles.

17. BIP (*Bitcoin Improvement Proposal*): Proposta de melhoria do Bitcoin é um documento para a introdução de recursos ou informações no Bitcoin. O BIP deve fornecer uma especificação técnica concisa do atributo e uma justificativa para a nova proposta de recurso. Esta é a maneira padrão de comunicar ideias, já que o Bitcoin não tem estrutura formal de organização. **O primeiro BIP (BIP 0001) foi enviado por Amir Taaki em 19/08/2011 e descreveu o que é um BIP.**

18. Bitcoin/bitcoin – Bitcoin: Quando grafado em letra maiúscula inicial, é usado para descrever o conceito do sistema ou a rede completa (*software* e *hardware*); bitcoin – em letra minúscula – é usado para descrever a unidade básica com a qual rede denomina movimentação e saldo em contas. É a moeda virtual mundial desenvolvida em código aberto e estrutura descentralizada e difundida pela Internet por indivíduo ou grupo utilizando o pseudônimo “Satoshi Nakamoto". Todas as transações realizadas são armazenadas em um banco de dados *on-line* e seus símbolos são ฿, BTC ou XBT. Atualmente, a menor fração do bitcoin é o centésimo milionésimo, denominado *satoshi*.

19. Bloco (*block*): Um bloco é um registro dentro da *blockchain* que contém e confirma várias transações em espera na *mempool*. Aproximadamente a cada 10 minutos, em média, um novo bloco com transações é anexado à *blockchain* por meio do processo de mineração.

20. *Blockchain*: A *blockchain* é um registro público de transações Bitcoin em ordem cronológica. A *blockchain* é compartilhada entre todos os usuários do Bitcoin. É usada para verificar o registro e a validade de transações Bitcoin e impedir gasto duplo.

21. *Block reward* (Recompensa de bloco**):** Refere-se aos novos bitcoins concedidos pela rede Bitcoin aos seus mineradores elegíveis para cada

bloco minerado com sucesso. Decai em 50% a cada 210.000 blocos, pelo mecanismo chamado *halving* ou *halvening*.

22. Burocracia virtual: Conceito cunhado por Olavo de Carvalho para a classe de indivíduos preparados para ocupar cargos na Administração, mas sem função, “seu único lugar possível na sociedade é no Estado, mas o Estado não tem lugar para eles”. Este grupo se diferencia da “geração nem-nem” pela expectativa específica de ingressar em postos do serviço público e é, em grande parte, explicado pelo “educacionismo”[450]. São rejeitados, inativos economicamente, que servem de idiotas úteis no conceito clássico leninista, defendendo interesses de burocratas apenas pela esperança de ocupar algum dia este papel.

23. Captura Administrativa (ou conhecida por Teoria da Captura): É um ponto fundamental do ramo da teoria da escolha pública conhecido como regulação econômica. A captura administrativa é uma forma de corrupção política que ocorre quando uma agência reguladora, criada para agir de acordo com o “interesse público”, age em benefício de interesses comerciais ou políticos de específicos grupos de interesse que dominam a indústria ou o setor daquela agência reguladora. A captura do regulador é uma forma de falha do Estado ao criar brecha para firmas ou grupos políticos atuarem de maneira prejudicial ao público, ou seja, produzindo externalidades negativas. Os órgãos são ditos “agências capturadas”.

24. Carteira (*wallet*): A carteira Bitcoin é o equivalente a um cofre ou carteira no mundo “legacy” que contém suas chaves privadas e permite que você gaste seus bitcoins efetivamente enviando-os a um novo endereço, geralmente do recebedor.

25. CBDC *(Central Bank Digital Currency)* – são moedas digitais emitidas por bancos centrais, sejam atreladas a uma moeda fiduciária (Yuan digital) ou *stable Commodity* (Petro Venezuelano). São uma etapa para eliminação de moeda alodial (numerário em espécie) e aumento de poderes estatais para aumentar base monetária, maximizando: a) efeito das reservas fracionárias (vez que TODOS os valores estarão depositados em alguma instituição); b) controle estatal (tanto de informação de quem transaciona com quem, como no poder de congelar ou invalidar saldos ou transações); c) capacidade de endividamento dos governos, impossibilitando a elisão ao juro negativo com saque em numerário; e, d) capacidade de políticas de “estímulos ao consumo”, com créditos com expiração para uso, como *vouchers* (dinheiro programável). O PIX é uma etapa para a implantação da

CBDC, reduzindo brutalmente privacidade dos usuários em troca de transações mais rápidas e "grátis" – e usam várias soluções comuns em criptos, como pagamentos por *QRcode*. O BCB promete desenvolver soluções de *smart contracts* e até reais digitais *offline* (como *smartcard* usado em transportes).

26. Chave pública *(Public key)*: Um conjunto de números e letras derivado matematicamente de uma chave privada. Você pode compartilhar sua chave pública para poder receber mensagens (com bitcoins) de outros usuários na rede.

27. Chave privada (*Private key*): Uma chave privada é um também conjunto de números e letras, uma combinação única de bytes de informação utilizada para assinar transações. Pense na chave privada como uma senha muito forte. As chaves privadas não devem ser compartilhadas jamais. Qualquer pessoa em posse da sua chave privada pode assinar transações e transferir a posse de seus bitcoins para outra chave privada.

28. *Cypherpunks*: É um grupo informal de pessoas interessadas em criptografia e privacidade.

29. *Cold storage* (Armazenamento a Frio): É uma carteira *off-line* usada para armazenar bitcoins. Com o armazenamento a frio, a carteira digital é armazenada em uma plataforma que não está conectada à Internet, protegendo a carteira contra acesso não autorizado, *hackers* cibernéticos e outras vulnerabilidades às quais um sistema conectado à Internet é suscetível.

30. *Confirmation* (confirmação): Confirmação significa que uma transação foi processada pela rede e é altamente improvável ser revertida. Transações recebem uma confirmação quando são incluídas em um bloco e a cada bloco subsequente. Mesmo uma única confirmação pode ser considerada segura para transações de baixos valores, apesar de que, em valores maiores como US$ 1.000, faz sentido esperar por 6 confirmações ou mais. Cada confirmação reduz exponencialmente o risco de uma transação ser revertida.

31. *Core developers* (Desenvolvedores principais): São os líderes do projeto. Propõem, avaliam e implementam melhorias, corrigem erros e estabelecem uma visão para o projeto, quando apropriado.

32. *Crypto*/cripto: Significa criptografada, oculta. Criptografia é o estudo de ocultar as coisas, a criptomoeda é a moeda criptografada.

33. Criptografia: A criptografia é o ramo da matemática que nos deixa criar provas matemáticas que fornecem um alto nível de segurança. Já sendo utilizada em comércio *on-line* e bancos. No caso do Bitcoin, a criptografia é utilizada para fazer com que seja impossível para qualquer um gastar fundos da carteira de outro usuário ou corromper a *blockchain*. Também pode ser utilizada para encriptar uma carteira, de modo que ela não pode ser utilizada sem uma senha.

34. *Crowdfunding* (Financiamento coletivo): Consiste na obtenção de capital para financiar um determinado projeto de interesse coletivo, em geral com participação de pessoas físicas interessadas na iniciativa.

35. Curva de Laffer: É uma representação teórica que afirma que, se as taxas de impostos aumentam acima de um certo nível, as receitas fiscais podem realmente cair, porque as taxas de impostos mais altas desencorajam as pessoas a pagar. Da mesma forma, a Curva de Laffer afirma que o corte de impostos poderia, em teoria, levar a receitas fiscais maiores.

***36. DAO* (*Decentralized Autonomous Organization*):** É uma organização cujas regras são especificadas através de programas de computador conhecidos como contratos inteligentes, os quais são executados e validados por uma *blockchain*.

37. Descentralizado: Manter um conceito fora do controle de uma única entidade e fazer com que a população geral trabalhe em conjunto como fator de controle.

38. Dissonância Cognitiva: Segundo a Teoria da Dissonância Cognitiva de Leon Festinger (1957), ocorre o fenômeno quando um indivíduo possui opiniões ou comportamentos incompatíveis com suas crenças - havendo elementos cognitivos sem coerência. Exemplo simples vem de a “Raposa e as uvas” de Esopo, em que a Raposa, por desejar algo inatingível, passa a criticar o objeto de desejo para reduzir sua dissonância.

39. Dividendo demográfico: Período, normalmente entre 20 e 30 anos, durante o qual as taxas de fertilidade e mortalidade caem e as populações têm o crescimento anormal na produtividade econômica devido ao pico na proporção de pessoas em idade produtiva (no Brasil, estima-se que o ápice da razão de dependência ocorra entre 2019 e 2022). Inverno demográfico: fenômeno percebido quando a taxa de natalidade se mantém em queda e a taxa de mortalidade mantém-se em níveis baixos. Isso tem como consequência o envelhecimento da população e a limitação das possibilidades de crescimento econômico. Segundo dados oficiais (IBGE),

as projeções indicam taxas de fecundidade em quedas sucessivas (6,21 em 1960; 4,07 em 1980; 1,81 em 2012; 1,74 em 2014 e projeção de 1,69 para 2016).

40. Dilema de Triffin (paradoxo de Triffin): É o conflito de interesses econômicos que surge entre os objetivos domésticos de curto prazo e os objetivos internacionais de longo prazo para países cujas moedas servem como moedas de reserva global. Esse dilema foi identificado na década de 1960 pelo economista belga-americano Robert Triffin, que apontou que o país cuja moeda é a moeda de reserva global, que as nações estrangeiras desejam manter, deve estar disposto a fornecer ao mundo um suprimento extra de sua moeda para atender à demanda mundial por essas reservas cambiais, levando a um *déficit* comercial. Para Robert Triffin, o sistema de Bretton Woods continha uma falha inerente e potencialmente fatal, ou seja, sua dependência em relação ao dólar, que deveria, conforme havia sido decidido em Bretton Woods, manter seu padrão-ouro.

41. *DYOR (Do Your Own Research*): Significa “faça sua própria pesquisa” e é uma frase comum utilizada na internet para que os usuários não caiam em desinformação, a frase se tornou muito usada por entusiastas de criptomoedas.

42. *Early adopter*: Alguém que é uma das primeiras pessoas a começar a usar um novo produto, especialmente uma nova peça de tecnologia.

43. Empréstimo Colateralizado: É um ativo que é dado como garantia de pagamento para uma obrigação de dívida. Por exemplo, no caso de uma hipoteca, o imóvel serve como colateral do empréstimo e, no mercado de criptomoeda, deixa uma quantia em crypto como garantia. Desta forma, o banco ou plataforma *crypto* possui uma garantia em caso de não cumprimento do devedor.

44. Efeito Cantillon: Os primeiros a receber o dinheiro recém-criado por um Banco Central veem sua renda subir, enquanto os últimos a receber o dinheiro veem seu poder de compra declinar.

45. Efeito *Dunning-Kruger*: Explica por que pessoas de baixo QI e conhecimento se sentem confiantes e capazes de emitir opiniões, viés cognitivo de ilusória superioridade.

46. Efeito Rede: É um fenômeno pelo qual um número crescente de pessoas ou participantes melhora o valor de um bem ou serviço. A Internet é um exemplo do efeito de rede. Inicialmente, havia poucos usuários na Internet, uma vez que era de pouco valor para qualquer pessoa fora do

exército e para alguns pesquisadores. No entanto, à medida que mais usuários obtinham acesso à Internet, eles produziam mais conteúdo, informações e serviços. O desenvolvimento e aprimoramento de *sites* atraíram mais usuários para se conectarem e negociarem entre si. À medida que a Internet experimentava aumento no tráfego, ela oferecia mais valor, levando a um efeito de rede.

47. Efeito Lindy: É o conceito de que o futuro da expectativa de vida de algumas coisas não perecíveis, como uma tecnologia ou uma ideia, é proporcional à sua idade atual, de modo que cada período adicional de sobrevivência implica uma maior expectativa de vida restante. Logo, quanto mais antigo algo for, mais tempo provavelmente existirá no futuro. De acordo com o Efeito Lindy, como o bitcoin existe há cerca de 10 anos, podemos esperar que ele continue por mais 10 anos. A cada ano a mais que ele sobrevive, mais tempo podemos esperar que ele esteja por aí no futuro. Como Taleb nos diz, a robustez de algo é proporcional à sua vida. Quanto mais tempo sobrevive, maior é a probabilidade de continuar a sobreviver.

48. Endereços: Equivalente à conta de um banco, informação necessária para envio de bitcoin, derivado da chave pública. **Existem 3 tipos de endereços no Bitcoin** Bech32 (*Segwit* Nativo) que começam com bc1. **Ex.:** bc1qar0srrr7xfkvy998745ydnw9an59gtzzwf9mdq. **Situação:** Compatível somente com carteiras que aceitam *segwit*. Dessa forma, uma carteira antiga pode não reconhecer fundos enviados a partir desse endereço. **Obs.:** Oferece as menores taxas possíveis. **Endereços:** *P2SH (Pay-to-Script-Hash, Segwit*). **Início:** Começam com 3. **Ex.:** 3K965KmP1Z73CnmQviecrnyiWrnqRhWXuA. **Situação:** Endereço de transição: Melhor opção para a maior parte dos usuários por ser compatível com todas as *wallets*. **Obs.:** Baixas taxas de transação. **Endereços:** ***P2PKH Legacy*** **(*Pay-to-PubkeyHash*, não *segwit*). Início:** Começam com 1. **Ex.:** 1OvyeornyiWrnqRhWXuAK965KmP1Z73CNm. **Situação:** Endereço antigo: Endereço compatível com todas as *wallets*.

49. *Exchanges* (corretoras): Uma “corretora” de criptomoedas, ou uma troca de moeda digital, é uma empresa que permite aos clientes negociarem criptomoedas ou moedas digitais por outros ativos, como moeda fiduciária convencional ou outras moedas digitais.

50. *Equity tokens* (*token* de patrimônio): Os *equity tokens* funcionam mais como um ativo de *stock asset.* Em outras palavras, os detentores de *tokens* de patrimônio possuem alguma forma de propriedade em seus

investimentos. Seus *tokens* representam quanta porcentagem de propriedade eles realmente possuem. Na maioria dos casos, os *tokens* de patrimônio representam um ativo, propriedade ou empreendimento de terceiros. Os *equity tokens* vêm em muitas formas: *Stocks*, Contratos Futuros, Opções, *Tokenized Real Estate* e *Tokenized Ventures*.

51. Efeito Gell-Mann: Em um discurso em 2002, Crichton cunhou o termo efeito da amnésia de Gell-Mann. Ele usou esse termo para descrever o fenômeno de especialistas acreditarem em artigos de notícias sobre tópicos fora de suas áreas de especialização, mesmo depois de reconhecerem que artigos dentro de suas áreas de especialização escritos na mesma publicação estão cheios de erros e mal-entendidos. Ele explica a ironia do termo dizendo que surgiu "porque uma vez eu discuti isso com Murray Gell-Mann, e ao mencionar um nome famoso, dou maior importância a mim mesmo e ao efeito do que o faria de outra forma."

52. *Faucets* (Torneiras): Uma torneira de bitcoin é um sistema de recompensa, na forma de um *site* ou aplicativo, que distribui recompensas na forma de um *satoshi*, que é um centésimo de um milionésimo de BTC, para os visitantes reivindicarem em troca de concluir um *captcha* ou tarefa, conforme descrito pelo *site*.

53. *Fork (soft fork e hard fork):* *Fork* é uma ramificação de uma rede de moedas, pode ser uma atualização ou nova versão. Se for retrocompatível, é *soft fork*; se não for retrocompatível, é *hard fork* – como os *forks* que resultaram no *bitcoin cash*, *bitcoin gold* e demais novas moedas que reconheceram blocos do bitcoin até certo ponto rodando seu próprio cliente incompatível (com suas próprias regras) depois.

54. *Fees*: O valor pago a um minerador para incluir uma transação em um bloco.

55. Gasto duplo: É uma possível causa de falha de sistemas de criptomoedas. O gasto duplo acontece quando um usuário consegue gastar as mesmas moedas digitais mais de uma vez. Diferentemente de moedas físicas, arquivos digitais podem ser duplicados, logo, o ato de gastar uma moeda digital não implica uma transferência de posse da mesma para outra pessoa. Portanto, é necessário que outros meios sejam utilizados para prevenção contra o gasto duplo.

56. Generais Bizantinos: Em computação, o Problema dos Dois Generais é um experimento mental para ilustrar as armadilhas e desafios de

planejamento na tentativa de coordenar uma ação através da comunicação sobre um ato não confiável.

57. *Gold Standard* (padrão-ouro): É um sistema monetário no qual a unidade de conta econômica padrão é baseada em uma quantidade fixa de ouro. O padrão-ouro foi amplamente utilizado no século XIX e no início do século XX. A maioria das nações abandonou o padrão-ouro como base de seus sistemas monetários durante o século XX, embora muitos ainda mantenham reservas de ouro substanciais.

58. Geração nem-nem: O termo refere-se à população jovem fora do mercado de trabalho e de instituições educacionais.

59. *Halving (halvening):* É um ajuste que ocorre na rede do Bitcoin e que reduz pela metade a recompensa dos mineradores, o que tem como consequência um corte na oferta de novas criptomoedas. E isso garante a característica deflacionária deste ativo.

60. *Hash/hashing:* Também conhecido como ID da transação ou txID, é um identificador único que pode ser usado em qualquer explorador de blocos para buscar por detalhes públicos de uma transação específica. Toda transação feita *on-chain* tem um *hash* único composto por vários caracteres alfanuméricos. Todo *hash* é único e derivado das informações da transação. Uma função *hash*, como as funções *hash* usadas para criar os diferentes tipos de endereços, é um algoritmo que mapeia dados de comprimento variável e os converte em dados de comprimento fixo. Os valores retornados por uma função *hash* são chamados de *hashes* e eles servem para compactar dados e assegurar a integridade dos dados transmitidos.

61. *Hashrate* (taxa de *hash*): A taxa de *hash* é a unidade de medida do poder de processamento da rede Bitcoin. A rede Bitcoin deve fazer operações matemáticas intensivas para fins de segurança. Quando a rede atinge uma taxa de *hash* de 10 Th/s, significa que ela pode processar 10 trilhões de cálculos por segundo.

62. *Hash*: Uma função que mapeia dados de comprimento variável em dados de tamanho fixo. Usado para identificar transações, blocos, calcular endereços e minerar blocos.

63. *Hodl* (*holdlers*): Um erro de escrita cometido por um usuário do pioneiro fórum Bitcointalk durante a *bull run* de 2013, que escreveu a palavra *Holding* (segurar) de forma errada, *Hodling*. Surgiu então o verbo "*to hodl*". *Hodler* é uma pessoa que não vende e segura seus bitcoins independente se o preço subir ou cair.

64. ***Hedge*** **(Cobertura):** É uma estratégia de proteção para os riscos de um investimento, que neutraliza a posição comprada ou vendida contra o risco de grandes variações de preço de um determinado ativo. Ao fazer uma operação de *hedging*, o investidor tem como objetivo eliminar a possibilidade de perdas futuras.

65. ***Hard money*****:** Moeda forte, moeda com boa cotação cambial.

66. ***Hardware Wallet:*** Um dispositivo relativamente seguro e prático (como *Ledger, Keepkey* e *Trezor*) para armazenar e assinar transações, protegendo as chaves privadas de transações.

67. Hiperbitcoinização: Esse fenômeno pode ser mais observado primeiramente em economias emergentes e subdesenvolvidas. O bitcoin se torna(rá) um refúgio seguro frente aos descompassos do Estado que causa crises financeiras: colapso das moedas nacionais, hiperinflação, colapso das dívidas nacionais.

68. ***HFSP (Have fun staying poor):*** A frase significa "Divirta-se ficando pobre. Frase que virou um "meme" como uma resposta a alguém que acabou de vender bitcoin ou disse que nunca consideraria comprar bitcoin.

69. ***ICO*** **(*****Initial coin offering*****):** Uma oferta inicial de moedas (*ICO*) é o equivalente do setor de criptomoedas a uma oferta pública inicial (IPO). As *ICOs* funcionam como uma maneira de arrecadar fundos, em que uma empresa que busca arrecadar dinheiro para criar uma nova moeda, aplicativo ou serviço lança uma *ICO*. Os investidores interessados podem comprar a oferta e receber um novo *token* de criptomoeda emitido pela empresa. Esse *token* pode ter alguma utilidade no uso do produto ou serviço que a empresa está oferecendo ou pode representar apenas uma participação na empresa ou no projeto.

70. ***IOUs*** **(*****"I owe you"*****):** É geralmente um documento informal que reconhece uma dívida. Um *IOU* difere de uma nota promissória, pois um *IOU* não é um instrumento negociável e não especifica termos de reembolso, como o horário do reembolso. Os *IOUs* geralmente especificam o devedor, o valor devido e, às vezes, o credor.

71. Impersonificação: Deixar de possuir qualidades, características ou aspectos de pessoa; fazer com que alguém ou si mesmo deixe de possuir qualidades pessoais. Etimologia (origem da palavra *impersonificar*). Im + personificar. (Dicionário *on-line* de Português).

72. KYC **("*****know your customer*****"):** política financeira de exigir identificação do cliente, apresentação de documentos e até com

reconhecimento facial, de voz e de digitais.

73. Lei de Gresham: A Lei de Gresham resume-se na seguinte oração: É um princípio econômico que diz que uma moeda sobrevalorizada (tem um valor determinado por uma autoridade monetária acima do de mercado) expulsa uma moeda subvalorizada (tem um valor determinado pela mesma autoridade abaixo do de mercado). Por exemplo, nos padrões bimetálicos, a prata circulava mais e o ouro era mais entesourado; ou, como hoje na Venezuela, em que os bolívares têm alta velocidade e os dólares são guardados como reserva de valor.

74. Lei de Amara: O cientista Roy Charles Amara definiu uma regra que encoraja todos a pensar um pouco mais sobre a tecnologia. A lei diz que "Tendemos a superestimar o efeito de uma tecnologia no curto prazo e a subestimar seu efeito no longo prazo". Ou seja, temos a tendência de ficar extremamente entusiasmados com as novas tecnologias e nossas expectativas inicialmente superam a realidade. Porém, eventualmente, essa dinâmica muda e começamos a subestimar o impacto que uma tecnologia terá.

75. Lei de Metcalfe: A lei de Metcalfe afirma que o efeito de uma rede é proporcional ao quadrado do número de usuários conectados no sistema (n^2). A lei caracteriza muitos dos efeitos de rede de tecnologias de comunicação e redes como a Internet, redes sociais e a *World Wide Web* e também a rede Bitcoin (com base no número de usuários ativos).

76. Lei de Wagner: Também conhecida como a lei do aumento da despesa do Estado. A lei de Wagner sugere que um Estado Social evolui de capitalismo de livre mercado, devido ao fato de a população exigir cada vez maiores serviços sociais. Os neokeynesianos e os socialistas muitas vezes exortam os governos a imitar Estados de Bem-Estar modernos, como a Suécia. A despesa pública aumenta constantemente, mostrando uma tendência ascendente. Tal lei prevê que o desenvolvimento de uma economia industrial será acompanhada por um aumento da percentagem da despesa pública no Produto Interno Bruto: "O advento da sociedade industrial moderna resultará no aumento da pressão política para o progresso social e aumento da provisão para créditos de consideração social pela indústria."

77. Lei de Michels ou Lei da Oligarquia: afirma que democracia e organização de grande escala são incompatíveis, confirmando a falsidade da "Teoria do interesse público".

78. Lei de Moore: É uma observação e projeção de uma tendência histórica relacionada à indústria de microchips e processamento de computadores. Foi observada por Gordon E. Moore, e consiste na previsão de que o número de transistores dos chips teria um aumento de 100%, pelo mesmo custo, a cada período de 18 meses.

79. Lei de Gall (*Gall's Law*): "Um sistema complexo que funciona invariavelmente evoluiu de um sistema simples que funcionava. A proposição inversa também parece ser verdadeira: um sistema complexo projetado do zero nunca funciona e não pode ser feito para funcionar. Você tem que começar de novo, começando com um sistema simples de trabalho." John Gall

Outra lei que o Bitcoin respeita é a *Gall's Law.* O Bitcoin é muito simples. Ele minimiza o número de variáveis dinâmicas. Novos sistemas complexos são incrivelmente difíceis de projetar do zero.

Um processo é bom quando não se trata de construir sistemas complexos do zero. Comece com um sistema simples que funcione e aprimore-o. Como alternativa, pegue um conjunto de subsistemas que estão funcionando (pequenos) e os componha, mas certifique-se de que a composição em si não se torne complexa, pois isso também não funcionará. Desenvolva iterativamente em pequenos passos e frequentemente certifique-se de que o resultado ainda está funcionando.

80. *Legacy System* (sistema legado): O termo "sistema legado" descreve um sistema antigo que permanece em operação em uma organização.

81. *Long e Short*: É uma estratégia que consiste em uma operação casada, na qual um investidor mantém uma posição vendida em um ativo (ação/criptomoeda) e comprada em outro no intuito de obter um residual financeiro da operação quando liquidá-la. Esta operação permite alavancagem financeira, pois é lastreada com margens de garantia.

82. *Lending / Marging lending* (empréstimo): O empréstimo de criptomoeda é a situação em que os investidores podem usar seus ativos cripto como garantia para obter um empréstimo fiduciário ou *stablecoin*, enquanto os credores fornecem os ativos necessários para o empréstimo a uma taxa de juros acordada.

83. Mineração: é o processo de utilização de computadores para realizar cálculos matemáticos para confirmar as transações da rede Bitcoin e aumentar a segurança. Como recompensa por seus serviços, os mineradores de bitcoin podem receber as taxas das transações confirmadas, além de

novas moedas criadas em cada bloco. A mineração é um mercado especializado e competitivo em que os benefícios são partilhados de acordo com o número de cálculos que são realizados. Nem todos os usuários bitcoin são mineradores e não é uma maneira fácil de ganhar dinheiro.

84. *Miner fee* (Taxa de mineração) / *Trasaction fee* (Taxa de transação): São pequenas quantidades de bitcoin concedidas para incentivar os mineradores de bitcoin a confirmar transações de bitcoin. Os mineradores de bitcoin são peças importantes que confirmam e protegem as transações na rede de Bitcoin. As taxas dos mineradores pagam aos mineradores pelo serviço que prestam.

85. *Mempool*: O grupo de transações esperando para serem incluídas em um bloco por um minerador.

86. Mercado futuros: Um contrato de futuros é um acordo legal para comprar ou vender um determinado ativo sendo ele commodity ou título a um preço predeterminado em um momento específico no futuro.

87. *Multisig*: A assinatura múltipla é uma configuração de carteira que pode exigir mais de uma chave privada para autorizar uma transação.

88. Moeda fiduciária (*Fiat*): É a moeda legal de qualquer país em que é impressa e emitida pelo governo via Banco Central. Moeda fiduciária é qualquer título não conversível, ou seja, não é lastreada a nenhum metal (ouro, prata) e não tem nenhum valor "intrínseco". Seu valor advém da confiança que as pessoas têm em quem emitiu o título.

89. Monerização: monerizar é aumentar fungibilidade e privacidade (do *token* ou da rede), saldos de bitcoin na *liquid/lightning* seriam "monerizados", ou o próprio Bitcoin estaria se aproximando aos atributos do monero ao adotar *Taproot* e outras melhorias de fungibilidade e privacidade.

***90. Network computer* (Rede de computadores):** Ou Rede de dados, na informática e na telecomunicação é um conjunto de dois ou mais dispositivos eletrônicos de computação (ou módulos processadores ou nós da rede) interligados por um sistema de comunicação digital (ou link de dados), guiados por um conjunto de regras (protocolo de rede) para compartilhar entre si informação, serviços e, recursos físicos e lógicos.

***91. Node* (nó):** Um *node* é um participante ativo e soberano da rede *P2P* do Bitcoin. Existem dois tipos de *node*: *full node* (nó completo), um nó que

carrega uma cópia completa da *blockchain*, e *pruned node* (nó cortado), um nó que tem apenas os últimos blocos da rede bitcoin. Ambos os nodes validam transações e propagam as transações pela rede, além de ter *mempool*. A única diferença é que o nó *pruned* não tem os blocos mais antigos da rede para ajudar na sincronização inicial dos blocos por novos nós entrando na rede.

92. Noob/newbie**:** calouro, iniciante.

93. NGU (Number go Up) Technology: Foi cunhado pelo famoso *bitcoiner* Pierre Rochard no twitter: "Bitcoin é a tecnologia NGU mais avançada do mundo." Isso quer dizer que os recém-chegados elevam a quantidade de usuários utilizando a rede bitcoin, ao passo que o preço do ativo também aumenta. A tecnologia *Number Go Up* expandido a sua abordagem também se refere a extrema escassez do bitcoin e a incapacidade de copiar seu efeito rede, isso resulta no aumento do preço do Bitcoin ao passo que outros atributos também aumentam como: quantidade de nós Bitcoin ativos; *Hashpower*; colaborações dos desenvolvedores; empresas provendo produtos e serviços; empregos gerados em todo ecossistema Bitcoin; números de transações; cobertura da mídia e FOMO; financiamento em projetos e desenvolvimento do Bitcoin.

94. Open source**:** *Software* de código aberto é aquele em que o código-fonte é disponibilizado e licenciado com uma licença de código aberto na qual o direito autoral fornece o direito de estudar, modificar e distribuir o *software* de graça para qualquer um e para qualquer finalidade.

95. On-chain (dentro da cadeia): As transações dentro da cadeia referem-se às transações de criptomoeda que ocorrem na *blockchain* - isto é, nos registros do *blockchain*, e permanecem dependentes do Estado da *blockchain* para sua validade. Todas essas transações em cadeia ocorrem e são consideradas válidas apenas quando da *blockchain* é modificado para refletir essas transações nos registros/livro de razão público.

96. Off-chain (fora da cadeia): As transações fora da cadeia referem-se às transações que ocorrem em uma rede de criptomoedas que movem o valor para fora da *blockchain*. Devido ao seu custo zero/baixo, liquidação imediata e maior anonimato, as transações fora da rede estão ganhando popularidade, especialmente entre grandes *exchanges*.

97. OTC – Over The Counter **(Mercado Balcão):** É a situação em que investidores profissionais, fundos, empresas e pessoas compram e vendem um ativo em grandes quantidades fora da *Exchange*.

98. P2P **(*Peer-to-peer)*:** É uma arquitetura de redes de computadores em que cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central. No caso do Bitcoin, a rede é construída de modo que cada utilizador transmita as transações de outros.

99. Pirâmides / *Ponzi Scheme* (esquema Ponzi): É um esquema com operação fraudulenta sofisticada de investimento do tipo esquema em pirâmide que envolve a promessa de pagamento de rendimentos anormalmente altos aos investidores à custa do dinheiro pago pelos investidores que chegarem posteriormente, em vez da receita gerada por qualquer negócio real. No Brasil, até a participação é criminalizada desde a Lei 1.521/51, art. 2, IX (pichardismo e equivalentes).

100. Profecia autorrealizável: Prognóstico que provoca sua própria concretização. Previsão que influencia o comportamento das pessoas de modo que acaba se realizando. Conceito de Robert Merton (1949). Muitas vezes é causado pelo "efeito manada", quando grupos se comportam de maneira semelhante sem organização planejada, seguindo o padrão da "massa crítica" - número mínimo de adotantes para sustentar ação.

101. *Proof of Brain* (prova de cérebro): medida de quanto de inteligência há em um ambiente ou projeto, aferida pela qualidade dos envolvidos e número e qualidade das contribuições nos repositórios.

102. *PoW (Proof of Work)*: Refere-se a uma porção dos dados que é difícil (consome muitos recursos e tempo) de ser produzida e extremamente fácil de verificar se atende alguns requisitos predeterminados. Produzir prova de trabalho pode ser um processo aleatório com baixa probabilidade de acerto, para que muita tentativa e erro (força bruta) seja requerida em média antes que uma prova seja gerada.

103. *PoS (Proof of Stake):* Prova de participação, normalmente com saldo vinculado ao nó.

104. *Pump and dump:* É um esquema de manipulação que envolve o aumento artificial do preço de um ativo por meio de declarações positivas falsas e enganosas (muitas vezes através de grupos do *telegram* ou relatórios de investimento), a fim de vender o ativo por preço mais alto (e algumas vezes recomprar depois de divulgação de notícias negativas, igualmente falsas ou fabricadas).

105. Preferência temporal: A preferência temporal é uma teoria em economia que trata a respeito da escolha de investimento e consumo de

bens em relação ao tempo. Os indivíduos estão sujeitos à passagem do tempo. Suas existências são finitas, seus corpos e mentes decaem. O tempo, portanto, é um fator escasso e, como tal, os indivíduos precisam economizá-lo.

106. Baixa preferência: Quando você possui visão de longo prazo. Ao não desfrutar de um bem no presente, a pessoa está disposta a algum sacrifício (poupar é sempre um ato de sacrifício) para adiar o usufruto desses bens no presente. Por isso, ao consumir pouco, a pessoa tem a preferência temporal baixa, nisso se permite que haja mais bens disponíveis para ser emprestados e aplicados em processos de investimento. Uma preferência temporal baixa gera uma maior abundância de bens livres para ser emprestados.

107. Alta preferência: Quando a pessoa possui visão de curto prazo. A pessoa se torna uma consumista, voltada sempre ao tempo presente e avessa à poupança. A escassez de capital é a consequência natural da alta preferência temporal das pessoas, traduzindo-se em um alto preço (juros) cobrado pelo uso do pouco capital que ainda resta.

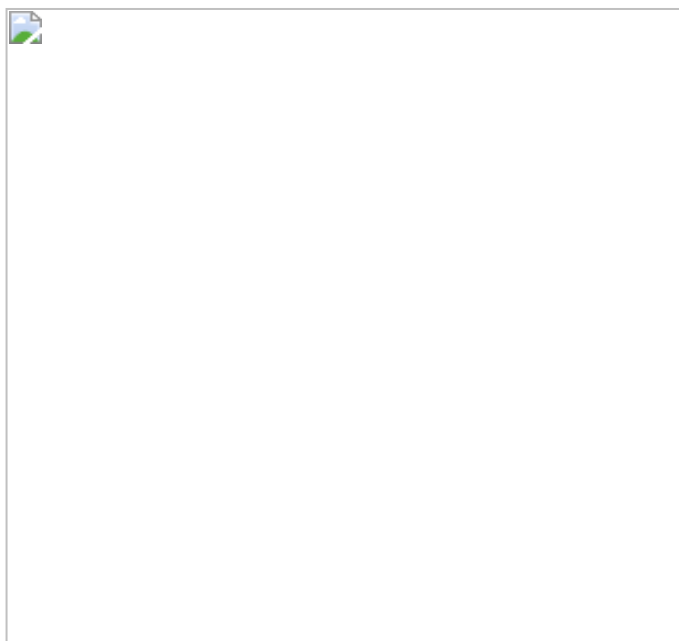
108. Ponerologia Política: É o estudo do mal, do grego *poneros* (malícia, maldade), é a ciência da natureza do mal adaptada a propósitos políticos. O termo foi cunhado pelo psiquiatra polonês Andrzej M. Lobaczewski, que estudou como os psicopatas influenciam no avanço da injustiça e como abrem caminho para o poder na política.

109. Problema de Olson (A Lógica da Ação Coletiva): A tese básica deste livro é a de que "mesmo que todos os indivíduos de um grupo grande sejam racionais e centrados em seus próprios interesses, e que saiam ganhando se, como grupo, agirem para atingir seus objetivos comuns, ainda assim eles não agirão voluntariamente para promover esses interesses comuns e grupais" (Olson, 1999, p. 14).

110. *Paper wallet*: Uma carteira *off-line* de armazenamento frio (*cold storage*), em que a chave privada é impressa em um pedaço de papel para armazenamento *off-line*. Era considerada uma das maneiras mais seguras de armazenar chaves privadas antes da criação de soluções de *hardware* e da implementação do *backup* a partir de *seed* (mnemônicos).

111. *Quantitative easing* (alívios quantitativos): A flexibilização quantitativa (QE) é uma forma de política monetária não convencional, na qual um Banco Central compra títulos de longo prazo no mercado aberto, a fim de aumentar a oferta de moeda e incentivar empréstimos e

investimentos. A compra desses títulos acrescenta mais dinheiro à economia e também serve para diminuir as taxas de juros, oferecendo títulos de renda fixa. Também expande o balanço do Banco Central. Quando as taxas de juros de curto prazo são iguais ou próximas a zero, as operações normais de mercado aberto de um banco central, que têm como alvo as taxas de juros, não são mais eficazes. Em vez disso, um Banco Central pode direcionar quantidades especificadas de ativos para compra. A flexibilização quantitativa aumenta a oferta de dinheiro comprando ativos com reservas bancárias recém-criadas, a fim de fornecer mais liquidez aos bancos.

112. Saylorização: processo de empresas abertas usarem juro negativo para comprarem bitcoin alavancado em vez de fazer recompra de ações, em processo de ataque especulativo contra *fiats*, fazendo até mesmo investidores de índices como SP500 se expor marginalmente a bitcoin.

113. *Smart contracts* (contratos inteligentes): É um contrato de execução automática com os termos do contrato entre comprador e vendedor sendo gravados diretamente em linhas de código. O código e os acordos nele contidos existem em uma rede *blockchain* descentralizada e distribuída. O código controla a execução e as transações são rastreáveis e irreversíveis. Os contratos inteligentes permitem que transações e acordos confiáveis sejam realizados entre partes anônimas e díspares, sem a necessidade de uma autoridade central, sistema legal ou mecanismo de

execução externo. Embora a tecnologia *blockchain* venha a ser pensada principalmente como a base do bitcoin, ela evoluiu muito além de sustentar uma criptomoeda.

114. *Slippage*: Refere-se à diferença entre o preço esperado de uma negociação e o preço pelo qual a negociação é executada. A derrapagem pode ocorrer a qualquer momento, mas é mais prevalente durante os períodos de maior volatilidade quando as ordens de mercado são usadas. Também pode ocorrer quando uma grande ordem é executada, mas não há volume suficiente no preço escolhido para manter o *spread* de compra / venda atual.

115. *Satoshi/sats*: A menor unidade divisível de um bitcoin. Cada unidade de bitcoin é composta de 100 milhões de *satoshis* (8 casas decimais). 1 *satoshi* (1 sat) = 0,00000001 bitcoin / 1 bitcoin = 100.000.000 de sats.

116. *Scam*: É um esquema fraudulento armado intencionalmente para enganar uma pessoa ou grupo de pessoas com objetivo de roubar dinheiro.

117. *Shitcoins*: É um termo pejorativo usado para descrever uma criptomoeda que se tornou inútil. É uma criptomoeda sem propósito, valor ou futuro.

118. Shitcoinheiro: Indivíduos que, por ignorância ou malícia, acumulam e/ou promovem tokens digitais sem valor. Muitos shitcoinheiros carecem de conhecimento nas áreas da economia austríaca, modelos de camadas de escala de protocolo, teoria dos jogos e ética. Muitos são propensos a explosões emocionais quando expostos à razão ou a perguntas difíceis sobre seus portfólios diversificados. Os passatempos incluem divertir-se se mantendo pobre e criar definições para maximalistas de Bitcoin no Urban Dictionary.

Steve ignorou o Bitcoin por anos e sente que perdeu o barco, apesar de seus amigos bitcoinheiros tentarem fazer com que ele acumulasse sats repetidamente. Para recuperar o tempo perdido, ele pulou na Coinbase e comprou todas as moedas de baixa capitalização na esperança de que um dia fosse o "próximo" Bitcoin. Steve é um cretino total. (By: BTC Sessions August 16, 2021).

119. *Sound money* (Dinheiro sonante): É aquele que não está sujeito a apreciação ou depreciação repentina do poder de compra no longo prazo, auxiliado por mecanismos de autocorreção inerentes a um sistema de livre mercado.

120. *Stablecoins:* É uma classe de criptomoedas que tenta oferecer estabilidade de preços e é garantida por um ativo de reserva (dólar, euro, ouro etc.). Os *Stablecoins* ganharam força ao tentar oferecer o melhor dos dois mundos, o processamento instantâneo e a segurança ou privacidade dos pagamentos de criptomoedas e as avaliações estáveis sem volatilidade de moedas fiduciárias.

121. Teoria das Escolhas Públicas: A escolha pública ou Teoria da Escolha Pública é um ramo da teoria econômica em que os conceitos da economia de mercado são aplicados à política e aos serviços públicos. Assim, na ciência política, a escolha pública critica a visão romântica de que o político é um servidor altruísta do interesse público em geral, substituindo-a por uma abordagem mais consentânea com o comportamento humano. Em vez de conceder aos políticos um tratamento especial, a escolha pública os trata como meros agentes humanos que priorizam a satisfação do seu próprio interesse.

121. *Testnet*: É uma rede separada com um *design* quase idêntico ao da rede Bitcoin para que os desenvolvedores possam testar melhorias e inovações sem colocar *satoshis* de verdade em risco.

122. UTXO: Acrônimo de "*Unspent Transaction Output*" (saída de transação não gasta) é uma moeda de bitcoin que pode ser usado como *input* (entrada) para ser gasto em transações futuras. Basicamente, é como os bitcoins que você possui e pode gastar são chamados dentro da rede Bitcoin. O saldo de uma carteira Bitcoin, por exemplo, é a soma de UTXOs controladas pelas chaves privadas daquela carteira.

123. xPub: Significa *"Extended Public Key"* (chave pública estendida). As chaves xPub são úteis porque o Bitcoin emprega o conceito de saídas de transação não gastas (UTXOs) em endereços de retorno. É a chave que gera todos os endereços, assim, podem-se obter todos os dados da sua carteira, transações anteriores e futuras. Mesmo que signifique "chave pública estendida", esta chave deve permanecer privada e nunca ser compartilhada.

124. *Welfare State* (Estado de bem-estar social): O Estado de bem-estar social, ou Estado-providência, ou Estado social, é um tipo de organização política, econômica e sociocultural que coloca o Estado como agente da promoção social e organizador da economia.

[1] Maximalistas - como *shitcoins* são testes de QI e BTC teste de fé no *legacy*: https://bit.ly/3Asikbq

[2] *Bitcoin Finance (BiFi)* vai ter *DeFi* e *CeFi*: https://atomic.finance/blog/a-sound-finance-manifesto/

[3] *RSK Network:* https://www.rsk.co/ / *Sidechain RSK - Convidada Solange Gueiros*: https://bit.ly/3sNzyfX

[4] *Liquid Network:* https://liquid.net/ / Tudo sobre a *Liquid*: https://bit.ly/38b3kC2

[5] *Lightning Network:* https://lightning.engineering/ / *LN* para iniciantes: https://bit.ly/2UTCECQ

[6] Exemplos do que estará no próximo volume: futurologia, descrição de conceitos de singularidade; disrupção; anapistão e justiça privada; mudança exponencial; economia da abundância; *digital dividel; seasteading* e *Citadel*, assim como, mecanismos e problemas de *smart contracts* (passados, atuais e potenciais) — *como os mercados decentralizados de apostas de morte; stables colateralizadas* como DAI do *maker DAO;* plataformas de apostas e serviços financeiros descentralizados e seus problemas intrínsecos; esquemas fraudulentos elaborados através de manipulação de mercado, *ICO*s ou *forks* maliciosos; consequências materiais e morais da hiperbitcoinização; natureza jurídica e econômica de *tokens* e minúcias das estratégias de *compliance;* gestão de riscos (inclusive com produtos criados com derivativos e futuros) e planejamento tributário e sucessório, ficam para o próximo volume.

[7] Comunismo é o polilogismo: https://bit.ly/3xa1ThS (arquivado: http://archive.today/hxCYX). E o progressismo atual depende de *behavioural bilingualism* (espécie de paralaxe cognitiva) para desmoralização e dessensibilização, como nas políticas de forçar uso de focinheira insalubre de pano que aumenta fómites e de confinamento de inocentes sem qualquer fundamento lógico ou empírico: https://bit.ly/2TyEvvV Mises denominava essa patologia "Complexo de Fourier": https://bit.ly/3dHN7Hz

[8] *Imposto = Roubo*: https://bit.ly/2SLF19H (arquivado: http://archive.today/8MLkN).

[9] *Legacy* é o sistema, em tecnologia, obsoleto, mas ainda operando, como a telefonia fixa.

[10] *Day Trading Bitcoin: Why 95% of Traders Lose Money and Fail*: https://bit.ly/3gnE1A9 (arquivado: https://archive.vn/DfLO1).

[11] Preço médio é *DCA* (*dollar cost averaging*), veja quanto teria hoje comprando 1 ou 10 ou US$100 por semana ou mês em BTC: https://dcabtc.com

[12] *Any Monkey Can Beat The Market:* https://bit.ly/3v7SVjx (arquivado: https://archive.vn/wYyJ8).

[13] Desde o Antigo Testamento, já se sabia que todos os retornos são proporcionais a esforços (Êxodo 22) e riscos (Eclesiastes 9:11-18).

[14] *Slippage*: https://bit.ly/3qS0bzC

[15] Ciclos civilizacionais: https://bit.ly/3wdzxSz

[16] Quem é John Galt?: https://bit.ly/3z8dnE2

[17] Medidas de dominância derivadas de *market cap* como o disponível no coinmarketcap.com não valem nada. Primeiro, que são listados centenas de ativos que não são *use tokens* (criptomoedas de uso) — lá são listados *equity tokens* (equivalente a uma ação) ou *stable coins* (*IOUs* colateralizados, em tese) e até mesmo *stable* bitcoins em outras plataformas; segundo,

que a maioria das *shitcoins* listadas tem valores e volumes descaradamente manipulados, sem qualquer quantidade relevante de volume em ordens.

[18] *Why BTC is the honey badger of money*: https://bit.ly/362H1NO (arquivado: http://archive.today/JOcCd).

[19] Se ciência não é mais método e sim consenso de comunidade, quando a comunidade está corrompida por concursos e seleções fraudadas e por distorções derivadas de financiamento governamental, então seu consenso não vale nada. Semmelweis, o primeiro a afirmar que lavar as mãos reduzia infecções, foi considerado louco e morreu no hospício, mesmo com demonstração empírica e publicações dentro dos padrões da época.

[20] A guilhotina de Hume cai na guilhotina: https://bit.ly/3ApvZjr

[21] Internado em hospício involuntariamente e morto no processo (Ignaz Philipp Semmelweis), resultou no *Semmelweis Effect* na psicologia comportamental: https://bit.ly/354nMmp (arquivado: https://archive.vn/3SeiS).

[22] Kelsen foi refutado por Voegelin (e, após isso, pela realidade e Lógica Argumentativa) - O dilema da Justiça natural: https://bit.ly/3dsiO7P (arquivado: http://archive.today/ORgoX).

[23] *Thank God for Bitcoin:* https://amzn.to/3xaQUog

[24] *Bitcoin: The Most Islamic Form of Money?* https://spoti.fi/3pE1BNe

[25] El Salvador tem primeiro presidente com *laser eyes:* https://bit.ly/3x7c5ra

[26] Como Saylor se refere aos *bitcoiners*: “Bitcoin é um enxame de vespas cibernéticas servindo a deusa da sabedoria, alimentando-se o fogo de verdade, exponencialmente cada vez mais inteligente, mais rápido e mais forte atrás de uma parede de energia criptografado” https://bit.ly/3xfYdvd *(twitter)*

[27] Thread Mises Capital vs Samy Dana: https://bit.ly/3ys87JQ / Com Bitcoin ultrapassando os R$ 233 mil, Samy Dana perderia hoje aposta contra Mises Capital (8 de fevereiro de 2021): https://bit.ly/3jpjwpA

[28] *Men Going Their Own Way:* https://bit.ly/3qLbdq9

[29] Bitcoin: https://en.wikipedia.org/wiki/Bitcoin

[30] *Wiki Bitcoin*: https://en.bitcoin.it/wiki/Main_Page

[31] *Bitcoin Revolution*: https://amzn.to/3v2oBXy

[32] IMB: https://www.mises.org.br/Ebooks.aspx?type=99

[33] Rothbard Brasil: https://rothbardbrasil.com/biblioteca/

[34] Inflação, base monetária e agregados: https://bit.ly/2Twp5Zf

[35] Os recentes eventos deixaram ainda mais claro: dinheiro de verdade é o ouro e você empobreceu: https://bit.ly/3532Yvs

[36] Quantidade de moeda criada – base monetária: https://archive.vn/dDRkU. Agregados monetários (quantidade de reais) triplicaram na década com queda de PIB real. Desde o início do Plano Real até 2019, *broad money* aumentou mais de 42x, entretanto, o Real só perdeu 97% do seu valor em ouro, originalmente R$11.5 o grama e hoje R$340,00 graças ao aumento de estoque de riqueza, que caiu na última década. Nesse caso, usamos os dados de “*broad money*” do Banco Mundial (M3 ou M4), "*narrow money*" seriam os M1 e M2. Para dados detalhados, vide relatórios do Banco Central na referência seguinte.

[37] 50% mais reais em 2020: https://bit.ly/351Oufs (arquivado: https://archive.ph/s8uP9)

[38] Estatísticas monetárias e de crédito do BCB: https://archive.ph/p3p6j

[39] Como governo gosta e precisa de inflação: https://bit.ly/3Be30ih

[40] *Whitepaper*: https://bitcoin.org/en/bitcoin-paper

[41] A mensagem é uma manchete do jornal britânico *The Times* de 3 de janeiro de 2009: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks* (*The Times 03/Jan/2009 "Chanceler à beira do segundo resgate aos bancos"*, tradução livre*).*

[42] *Satoshis' posts*: https://bit.ly/3g889k9

[43] *FRED data*: https://fred.stlouisfed.org/series/FYFSD

[44] "Curso forçado" consiste no dever legal de aceitar a moeda fiduciária estatal para qualquer pagamento, "*legal tender*", como escrito hoje nas cédulas onde havia "conversível por ouro".

[45] Base monetária global era de 94,8 trilhão de dólares em 2020 *(Only One Number Mattered to Global Markets in 2020):* https://archive.ph/6q8I3 em tempo real; *Fiat Market Cap:* https://fiatmarketcap.com/

[46] Alodial é sem vínculos ou ônus, como cédulas e contrário a saldo em banco.

[47] *An Escalating War on Cash*: https://bit.ly/3gkIoMs (arquivado: http://archive.today/7VOtg).

[48] Nota de 500 euros - Obs.: *Pararam de emitir essa nota, mas ainda é válida e circula.

[49] *Gold Reserve Act*: https://bit.ly/3hh2bhm

[50] "Qual o melhor investimento da década? Ouro lidera; Bolsa perde da inflação": https://archive.vn/3CGCR

[51] *Capital asset pricing model*: https://bit.ly/3whO13Q e VPL: https://bit.ly/3jFEam3

[52] Teoria da Captura Regulatória: https://pt.wikipedia.org/wiki/Captura_do_regulador

[53] Quarentena e Lockdown foram crimes contra a humanidade: https://bit.ly/2SQHcsE (arquivado: http://archive.today/Qf26W).

[54] *Main Street bailout failed:* https://bit.ly/2Ugd8qB

[55] Arthur C. Clark previu em 1964 a obsolescência das cidades em decorrência da viabilidade futura de comércio e serviços remotos: *Arthur C Clarke predicting the future in 1964-Trimmed.flv*: https://bit.ly/3yfPyZj

[56] Nascimentos em 2020 caem 5,66%: https://bit.ly/3zjsQ43 (Arquivado: http://archive.today/cMsl7)

[57] *Fertility rate:* https://data.worldbank.org/indicator/SP.DYN.TFRT.IN?locations=BR e uma análise aprofundada por Peter Zeihan: https://www.youtube.com/watch?v=EeGX105X7ac

[58] Conceito claro na "autorresponsabilidade" da filosofia objetivista: https://archive.vn/isrO1

[59] Diversos artigos indicam que até 60% dos homens entre 20-35 anos em países de primeiro mundo apresentam tendências "herbívoras" em decorrência das mudanças de papéis e valores sociais – perdem interesse em sexo, alimentação ou realizações materiais relacionadas a valores masculinos, identificados no "Código dos Homens" (Jack Donovan) (https://bit.ly/3xgOaWN) em força, coragem, destreza e honra: https://bit.ly/3qOz4VV – representando um risco à "armadilha malthusiana", situação de colapso civilizacional devido à estagnação tecnológica.

[60] Para entender que a maior parte do gasto de inteligência soviético era contra inteligência (subversão e desmoralização) vide Heitor de Paola, no *Eixo do Mal Latino-Americano e a Nova Ordem Mundial ou* Yuri Bezmenov https://bit.ly/3hvV1EX

[61] Para entender como a "pirâmide nutricional" recomendada pelo governo é parte da engenharia social ler "*The Fiat Standard*" do Saifedean ou: *What made the Ancient Egyptians Fat and Sick?* https://bit.ly/3BgBUa7

[62] Porque oligarcas bilionários são esquerdistas: https://bit.ly/3AcHryZ (arquivado: http://archive.today/s25br).

[63] Paralaxe Cognitiva: https://bit.ly/3wcXNEt (arquivado: http://archive.today/TNtxU).

[64] Demonstrando o conceito de religião política e o fato de que nunca houve real separação de religião e Estado e sim substituição da Igreja pela religião política (ou religião civil de Rousseau): https://archive.vn/HVwXE A voz do povo é a voz do diabo, a voz de Deus é a LEI natural e bíblica, Deus é a verdade (João 14:6) e tudo que não presta (ódio, inveja, vícios, crime, comunismo…) vem da mentira (João 8:44).

[65] *Idiocracy* (como motivações distorcidas podem levar a idiotização mundial): https://bit.ly/2XOF1I0

[66] *Paypal* bloqueia conta de Olavo de Carvalho por disseminação de *fake news*: https://bit.ly/3hArDNQ (arquivado: https://archive.vn/EkzAu).

[67] Hayek - Arrogância Fatal: https://bit.ly/2V4k5LU e o Uso do Conhecimento na Sociedade: https://bit.ly/3ykqfpn

[68] Expressão em inglês equivalente a "ter o seu c* na reta".

[69] Termo referido em clássicos como *Pense e Enriqueça*, de Napoleon Hill, e *Pai Rico*, *Pai Pobre*. Livros mais adequados para o contexto atual com o mesmo fito seriam *12 regras para a vida*, de Jordan Peterson, e *Rational Male*, de Rollo Tomassi.

[70] Dinheiro *versus* Moeda - *Hidden Secrets Of Money* Ep 1 - Mike Maloney https://bit.ly/3dIuvqT

[71] A evolução dos meios de troca no Novo Mundo ocorreu mais rápido que no Velho Mundo, mas na mesma ordem, demonstrando que é um processo natural.

[72] Bitcoin é a próxima etapa lógica na tecnologia do dinheiro: PlanB @100trillionUSD (Twitter).

[73] *The Problem of Social Cost*: https://bit.ly/3AqNmR1

[74] *Property rules, liability rules, And inalienability: one view of the cathedral. Harvard Law Review, 1972:* https://archive.vn/yh2bo

[75] Mais uma prova do "Neo Feudalismo" de Max Keiser e da infância mental é o documentário "Alquimia da Verdade", no qual um empresário é obliterado moral e financeiramente por perseguição estatal e ainda acha que vai encontrar restituição na (in)justiça estatal: https://bit.ly/3ApJ6Bl

[76] "*it is more or less impossible to reach Bitcoin maximalism while retaining any amount of trust in the system"*- Why The Yuppie Elite Dismiss Bitcoin: https://bit.ly/3h3BbSp (arquivado: http://archive.today/qUl1C) ou Por que os Faria Limers rejeitam o Bitcoin? https://bit.ly/3qHtRPJ (arquivado: http://archive.today/ktfJm).

[77] Ross Stevens, da NYDIG, explicando como gente com alto QI deixa de entender o BTC por falhas cognitivas de viés (em regra por acreditar em instituições falidas por terem funcionado no passado): *Ross Stevens - MacroMinds | NYDIG - The Beauty of Bitcoin:* https://bit.ly/3yfRIIp

[78] Quarto mês de pânico: onde estão as evidências? https://bit.ly/3yaHN7d (arquivado: https://archive.vn/qGF2b).

[79] Não há "ciência estabelecida" que corrobore o uso de máscaras: https://bit.ly/2TilrSw (arquivado: https://archive.vn/D41Ut).

[80] *Cumulative number of coronavirus-positive (COVID-19) Cumulative number of coronavirus-positive (COVID-19) patients confirmed on Diamond Princess cruise ship docked in Japan as of April 16, 2020:* https://bit.ly/3he8hze

[81] *USS Theodore Roosevelt, COVID-19, and Ships: Lessons Learned: https://bit.ly/3hgG0rM (arquivado: http://archive.today/xflNN).*

[82] Evolução da Programação Web: https://bit.ly/3jHLRrU

[83] Engenheiro do google confessando manipulação das buscas nas Eleições de 2020, Vídeo produzido por *Project Veritas*: https://bit.ly/3qOkbTM

[84] Dilma se encontra com Zuckerbeg no Panamá: https://glo.bo/3dsT22Z (arquivado: http://archive.today/coVe4).

[85] China tem um plano para dominar a Internet do mundo todo: https://bit.ly/36dmPss

[86] Hitler tentando salvar o mundo, com conceitos socialistas totalmente errados: https://youtu.be/PQGMjDQ-TJ8

[87] O caminho da servidão: http://rothbardbrasil.com/wp-content/uploads/arquivos/caminhodaservidao.pdf

[88] ISTOÉ afirma que presidente "além de broxa deve ser gay passivo": https://bit.ly/3AnDkQF (arquivado: http://archive.today/xkbk2).

[89] Desnazificação é o processo de destruição (financeira, moral e política) das elites criminosas no final de regimes de exceção. Nos países comunistas que as elites burocratas não foram condenadas e punidas por seus crimes – como a Rússia, Ucrânia, Moçambique e Angola – as famílias desses burocratas continuaram sendo os donos dos países e mantendo suas vítimas em regimes de miséria e repressão. Compare os vizinhos Bielorrússia com Lituânia ou Letônia com triplo do PIB *per capita* e verá a diferença: *Why is UKRAINE the POOREST country in EUROPE? - VisualPolitik EN:* https://bit.ly/3mNrH1h

[90] Larápios do Covidão: https://bit.ly/3wkmkaB (arquivado: http://archive.today/M4SGw).

[91] Brasil tem anos seguidos de queda no consumo de energia: https://bit.ly/2UU6Xsv (arquivado: http://archive.today/Z11GP).

[92] Fuga de cérebros sem precedentes, demonstrando que com Bolsonaro a dominância oportunista foi ampliada: https://bit.ly/3xhMEU7 (arquivado: http://archive.today/bSmiH).

[93] José Dirceu: https://bit.ly/3jrtE1u (arquivado: http://archive.today/0A9zZ).

[94] Moro determinou prisão em sala de Estado Maior, com luxos sem precedentes nem previsão legal para Luiz Inácio: https://glo.bo/3heZcVE (arquivado: http://archive.today/3gagZ).

[95] Se o regulamento do SINARM acabou com critério subjetivo para autorização de compra de armas, ele adicionou mais de uma dezena de dispositivos desarmamentistas, como a proibição automática a depender dos índices de criminalidade na região, só os muito ricos podem ter arma no governo Bolsonaro, exatamente porque os seus indicados para o setor eram militantes progressistas: https://bit.ly/361uhXD (arquivado: http://archive.today/VLDnF).

[96] 14 leis feministas de Bolsonaro em menos de 2 anos: https://bit.ly/2SIbLRe (arquivado: http://archive.today/wdcn2) e a 15# foi a Lei 14.188 que institui crime com tipo aberto de “violência psicológica”.

[97] Página da redação vazada, gráfica sem licitação, confusão no gabarito e erros em notas – sem contar conteúdo progressista militante: https://archive.vn/vzuyc considerado o mais vergonhoso internacionalmente: https://archive.vn/79XXR

[98] Bolsonaro se submete a ditadura comunista mais assassina da História: https://bit.ly/2UOHCQJ (arquivado: http://archive.today/GpLvX).

[99] Armadilha da dependência: https://bit.ly/3AeOK9h arquivado: http://archive.today/sjvWw

[100] 66 milhões: https://glo.bo/3x9oI5x arquivado: http://archive.today/o1hDI

[101] *The complicated truth about China's social credit system* https://bit.ly/3jhY31J (arquivado: http://archive.today/GsiAl)

[102] *Organ harvesting* ("doações involuntárias" de órgãos de dissidentes): *How to Make Money in China: Selling People’s Organs:* https://bit.ly/3hfhXJH

[103] A patente do número Pi: https://bit.ly/3dDXEU0

[104] Há muito material no *YouTube* deles – embora muitas coisas que defendem sobre o *legacy* (sistema convencional) e seus envolvimentos com empresas com baixa admiração na comunidade (XDEX/Atlas) sejam polêmicas, sendo acusados de serem Faria Limers.

[105] Roteiro de estudos com link para recursos: https://bit.ly/3w8Ixt9

[106] Estado é escravidão? Paulo Kogos: https://bit.ly/3vcOILo

[107] KoreacomK: https://twitter.com/KoreaComK

[108] Fontes em inglês devem incluir: @PeterLBrandt @alessiorastani @tonevays @chrisdunntv, BlackpillBr (https://t.me/bitcoinblackpill_BR) e Raicher (https://t.me/nostreidamos)

[109] Introdução indefectível: https://bitcoinheiros.com/intro-bitcoin/

[110] Futuro descentralizado: https://bit.ly/3v8HyYL

[111] Redes de confiança formais e informais: https://bit.ly/3iwirwi

[112] Uma rede de confiança *(WoT – web of trust)* é um grafo que estabelece uma relação de confiança entre duas partes, mesmo que elas não se conheçam previamente, através de ligações diretas ou indiretas: https://bit.ly/3h52vzN (Arquivado: https://archive.vn/dgHRu) .

[113] MOOC grátis da Universidade de Nicosia: https://www.unic.ac.cy/blockchain/free-mooc/

[114] *Data-Secrecy Export Case Dropped by U.S.Jan. (12, 1996):* https://nyti.ms/2UOKWeF (arquivado: https://archive.vn/GSjk0) / O criador do PGP: https://bit.ly/3hb25bb / https://pt.wikipedia.org/wiki/Phil_Zimmermann

[115] Asimov sobre 2020 e *digital divide*: https://www.youtube.com/watch?v=-_4xkkIKW2c muitos futurólogos estudam cenários de "economia da abundância" (Kurzweil) ou "sociedades pós escassez" (Isaac Arthur): https://www.youtube.com/watch?v=_Kt7883oTd0

[116] *The Saylor Series*: https://bit.ly/2SMmutV

[117] Vide *FAANGs* - Facebook (FB), Amazon (AMZN), Apple (AAPL), Netflix (NFLX), and Alphabet (GOOG) *versus* S&P500.

[118] Uma interpretação particular da hierarquia das necessidades particulares em homens e mulheres, sob uma perspectiva *MGTOW*: https://bit.ly/2SK2yHV

[119] 12 camadas da personalidade: https://bit.ly/3qDKXhC

[120] *Rankings* de QI do Wikipédia e exames do Pisa.

[121] *Open borders IQ and civilization:* https://bit.ly/3jFVFCD

[122] Se pretende ter filhos, entenda o "teste do *marshmallow*" para entender como a baixa preferência temporal é mais determinante para o sucesso que QI. Mais importante ainda que autocontrole é planejamento para evitar as tentações (sem arriscar *esgotamento do ego)*: https://bit.ly/3wpzGCR

[123] *IQ and national success:* https://bit.ly/2UolWuI

[124] Como descrito por Lobaczewski na "Ponerologia Política", a patocracia é o sistema em que "todas as posições de liderança devem ser preenchidas por indivíduos com anomalias psicológicas" e que "seu nível intelectual ou habilidades profissionais não devem ser levados em consideração" e que sua consequência é "Sob tais condições, nem uma área da vida social pode se desenvolver normalmente, seja na economia, cultura, ciência, tecnologia ou administração. A patocracia progressivamente paralisa tudo". Outra obra importante sobre o tema é *Mentalidade Esquerdista*, de Lyle Rossiter.

[125] Vide "*Shadow World"* de Robert Chandler e os clássicos "*1964, O Elo Perdido"*, de Vladimir Petrilak, e "*Desinformação*, de Ion Pacepa: Sobre as ações atuais de captura de elites e dirigentes políticos pela China, é recomendável assistir: https://bit.ly/3wfSpAz

[126] Foro de São Paulo e "Teologia da Libertação": https://bit.ly/3wkkqa6 para detalhes do acordo de 2019 entre Vaticano e Pequim para entregar cristãos para expurgos e garantir cardeais nomeados pelo partido comunista no próximo conclave vide Cardeal Zen: https://bit.ly/3Aoyym3 (o Papa argentino ser um agente infiltrado, explicaria o silêncio e colaboração da Santa sé dos crimes da ditadura mais assassina da História, promovendo genocídios em lugares diversos como Xinjiang, Mongólia Interior e Tibete). Até militantes de esquerda denominam o "acordo secreto" como "completo controle do PCC" (mencionando que as imagens de Jesus em igrejas tinham sido substituídas pelas de Mao, assim como a "Bíblia oficial" rescrita) e que seria em troca de US$2Bi/ano: https://bit.ly/3hbbOhM

[127] Indicador com 95% de sucesso em um ano, fazer o contrário do que recomenda a CNBC: https://bit.ly/3jHcBZi

[128] Curva de Rahn: https://en.wikipedia.org/wiki/Rahn_curve / Gasto público máximo para a curva de Rahn é entre 15-25% do PIB e curva de Laffer na Califórnia: https://bit.ly/3jHBd4v (arquivado: https://archive.vn/3dCvE).

[129] Efeminação dos valores, hedonismo, redução da fecundidade, diluição da moeda com aumento do assistencialismo são elementos comuns no colapso de diversas civilizações: https://bit.ly/3ABCJLs

[130] @Thaitata https://twitter.com/thaitata/status/1054576337351008256

[131] *The Red Pill (*documentário*)*: https://bit.ly/3jFfGJv

[132] Como funcionou a escravidão e os esquemas de promiscuidade obrigatória: https://www.youtube.com/watch?v=zkcVkmzeJ4U. e https://www.youtube.com/watch?v=_AS-5kceQ_A.

[133] *Iron Rules*: https://bit.ly/36bfh9H

[134] Stefan Molyneux: https://bit.ly/2RpKgLv

[135] *Welfare* destruindo fecundidade: https://bit.ly/3jBVSXv

[136] Hipergamia e poliginia são fatos etnobiológicos e não culturais e não são ignoradas pelas leis de família feministas que inviabilizam famílias, elas são usadas para destruir famílias, o exemplo ápice disso são os herbívoros (*herbs*) japoneses (pessoas jovens que desistem de buscar sexo ou relacionamentos): https://pt.wikipedia.org/wiki/Herbs e as mulheres pagando alto para ser inseminadas por desconhecidos: https://bit.ly/3yleKOx

[137] Porque homens não querem mais casar: https://bit.ly/3ylIP0p

[138] Mulher decide se vai ter sexo, homem se vai ter compromisso: https://bit.ly/3yl8WE8 (arquivado: http://archive.today/YthEH)

[139] Como explica o brocardo "uma chave que abre qualquer porta é uma chave mestra e a porta que se abre com qualquer chave uma arrombada", devido ao dimorfismo, mulher pode enganar homens sobre paternidade, mas o contrário não é possível: *Mater semper certa est*

[140] União com mulher alheia, mesmo repudiada sem culpa, é adultério e amaldiçoa por gerações: Mt19:9 "Eu vos digo, porém, que qualquer que repudiar sua mulher, não sendo por causa de prostituição, e casar com outra, comete adultério; e o que casar com a repudiada *também* comete adultério". Por isso se diz que as "mães solteiras" devem permanecer "solteiras" (se o casamento é o sexo, só existe mulher solteira se inseminada virgem) - e encerrando as leis feministas e de paternidade involuntária a maioria delas também deixariam de ser mães. A mulher, em muitos sistemas jurídicos pode escolher: 1) se fica fértil ou não; 2) se é coberta ou não; 3) se inseminada permite ou não nidação; 3) se mantém gravidez ou aborta; e, se parir, 4) se dá criança ou registra em seu nome - e o homem tem paternidade forçada apenas por DNA, quando não imposta até sem DNA, como nas teratologias de multiparentalidade e "paternidade afetiva involuntária".

[141] Dessa assimetria de poder entre homens e mulheres que resulta a explosão de filhos fora do casamento, mais vulneráveis ao crime, pobreza e submissão e com menos chances de desenvolvimento. Vide Stefan Molyneux, *The Truth About Single Moms:* http://www.fdrurl.com/single-moms-transcript (*The Truth About Single Moms*: https://bit.ly/3xbjINH)

[142] Gênesis 1:28 "Deus os abençoou: [Frutificai – disse ele – e multiplicai-vos, enchei a terra e submetei-a. Dominai sobre os peixes do mar, sobre as aves do céu e sobre todos os animais

que se arrastam sobre a terra]” demonstrando que a militância por "direitos dos animais" é demoníaca.

[143] Na França, há mais de 15 anos, é crime fazer DNA privado de seu filho para saber se é seu, no Brasil também já houve caso de justiça determinar paternidade involuntária diversas vezes (expressamente por motivo patrimonial, como no caso do goleiro Bruno): https://bit.ly/3dw6N0Z (arquivado: http://archive.today/YSglY).

[144] Por não compreenderem quais critérios os machos as avaliam, mulher por vezes se avalia segundo critério de valor para homens. Os homens são avaliados pela capacidade de prover segurança e as mulheres pela fertilidade e fidelidade que podem oferecer - e não por renda, independência ou formação acadêmica.

[145] “Filhotes não são bebês e [mãe de pet] não são mães”: https://bit.ly/3ApQU5Y sociedades que adoram animais, usualmente, sacrificam humanos inocentes. Direitos animais como subversão moral: https://bit.ly/368Fq9j

[146] Para entender comportamentos evolutivos ler o seminal “O Macaco Nu” de Desmond Morris, “O Gene Egoísta” de Dawkins ou *Tribalism and the fall of West:* https://bit.ly/3hz9n7K

[147] Princípio da não agressão (Daniel Fraga): https://bit.ly/3qKDQnh (Visão Libertária): https://bit.ly/3dGpdMt

[148] Geração Paulo Freire: exposição o “Cu é Lindo” na UFBA explica o resultado no Pisa. O que os universitários fazem hoje explica o resultado negativo do Brasil no Pisa, fruto de uma geração ideologicamente manipulada: https://bit.ly/36cqKG0 (arquivado: http://archive.today/cnIyq).

[149] Como o Estado destrói a família: https://bit.ly/3hiCFHz (arquivado: https://archive.vn/w1AXM).

[150] Escurecimento global: https://bit.ly/3AsyEJt

[151] Planeta Azul em Algemas Verdes: O que está em perigo: o clima ou a nossa liberdade?: https://amzn.to/3jGgcH6

[152] “O Estado não Conserva a Biodiversidade": https://bit.ly/3jBWwEp

[153] Desastre de Kyshtym: https://bit.ly/2SLIZiB

[154] Estimativas variam que entre 10 e 28 milhões de mortos de fome devido à matança dos pássaros na Campanha das Quatro Pragas: https://bit.ly/2UkEn3s

[155] Ambientalista Libertário: https://bit.ly/3Ddu1Ei

[156] *Gell-Mann amnesia effect: https://bit.ly/3wfzUMD*

[157] Os direitos naturais e lógicos derivam da liberdade (ou autopropriedade para Hoppe) como fato, inclusive de adquirir, de maneira originária ou derivada, outros direitos. Consentimento é legitimação e a diferença entre estupro e sexo e entre doação e furto. Direitos públicos negativos são aqueles que limitam ações do governo e direitos públicos positivos (de receber algo, como direito a educação e saúde) não podem ser prestados sem violar PNA, não sendo então legítimos.

[158] Convergência de *bitcoiners* (como Saifedean), Jordan Peterson e sua família e o médico recordista Shawn Baker a dietas carnívoras: *Carnivore Diet: Why would it work? What about Nutrients and Fiber?* https://bit.ly/3jGv4FG

[159] Pecuária salva o mundo. *Are Cows really Bad for the Planet?* https://bit.ly/3wfzWnJ

[160] *Democracy or Republic?* https://bit.ly/3hdGIpC (arquivado: http://archive.today/zD9SA). diversas frases indefectíveis dos pais fundadores em repúdio a democracia como *"Democracy is two wolves and a lamb voting on what to have for lunch. Liberty is a well-armed lamb contesting the*

vote!” Benjamin Franklin ou *“Remember, democracy never lasts long. It soon wastes, exhausts, and murders itself*” John Adams ou "*A democracy is nothing more than mob rule, where fifty-one percent of the people may take away the rights of the other forty-nine”* Thomas Jefferson.

[161] A relação conturbada entre os maximalistas e o obeso que recomenda jejum é detalhada em: https://bit.ly/2ThyYKm (arquivado: http://archive.today/uqEUE).

[162] Uma nova abordagem para os problemas de desenvolvimento: https://bit.ly/3dydrnp (arquivado: http://archive.today/BkIOb).

[163] *The Bitcoin Standard*, como *As seis lições*, também correlaciona o colapso de civilizações e nações com a diluição de valor de suas moedas, decorrente de *déficit* público: https://bit.ly/3x9Ou9K

[164] *Your nation's IQ matters*: https://bit.ly/3hwxmo2

[165] Assim, aquelas pessoas que tenham uma baixa preferência temporal, estarão dispostas a renunciar a bens presentes em troca de conseguir bens futuros com um valor não muito maior, e efetuarão trocas entregando seus bens presentes a outros que tenham uma preferência temporal mais alta, e portanto, valorizem com mais intensidade relativa o presente do que o futuro…

Democracia e empobrecimento segundo Hans-Hermann Hoppe: https://bit.ly/3ymEtGe / (arquivado: http://archive.today/DFdAP).

Preferência temporal: https://bit.ly/2SMHMaP

[166] Embrapa: https://www.cnpm.embrapa.br/projetos/gite/

[167] Geração Nem-Nem+: uma bomba-relógio: https://bit.ly/2UgwrjH (arquivado: https://archive.vn/2ISHt).

[168] Mateus 20:1-16: Parábola dos Trabalhadores das Vinhas

[169] *Should We End the Fed?* https://bit.ly/2TpNm3j

[170] Murray Rothbard em *Manifesto Libertário*. Um panorama atualizado é dado pelo *bitcoiner* Max Keiser em seu Keiser Report (da russa RT), informando com dados oficiais como: 1) a maioria dos universitários não aumentam sua capacidade mental no curso (e muitos até perdem inteligência e habilidades); 2) como há mais que o dobro de formandos que demanda por formados, resultando em 3) na maioria dos graduados executando profissões que não demandam formação, tendo na universidade investimento perdido, com altíssimo custo de oportunidade: https://bit.ly/3jFh1jr

[171] Lei de Ferro da Oligarquia: https://bit.ly/38dwNv0

[172] Como bem lembrado na Revolta de Atlas “basta criar leis que não podem ser cumpridas e faturar em cima dos culpados”. Por que existem tantas leis no Brasil: https://bit.ly/3srAjLr

[173] *Curley Effect*: https://bit.ly/3AnMQTT

[174] Estados totalitários como a Coreia do Norte ou Cuba (que proíbem ou restringem o acesso de seus escravos/cidadãos à Internet) podem continuar existindo após o fim dos Estados Sociais – até que os mercados de apostas de morte sejam totalmente desenvolvidos e a caridade financie a eliminação dessas ditaduras. Plataformas de apostas descentralizadas de morte já eram concebidas e formalizadas em 2004 como consequência de *criptos* alodiais, antes mesmo do conceito de *smart contracts: Assassination Politics (by Jim Bell)* https://cryptome.org/ap.htm *(arquivado: http://archive.today/nnPBI)*

[175] *Fork* é divisão de sistemas.

[176] Versão em português: https://bit.ly/3yo0zIm (arquivado: https://archive.vn/meIQi).

[177] Who is Satoshi? https://bit.ly/3gAqeai

[178] Tim May, *The Crypto Anarchist Manifesto*: https://bit.ly/2Tmpcqd (arquivado: https://archive.vn/7VfHH).

[179] Por que Satoshi se ausentou e como: https://bit.ly/3hlHPT1 (arquivado: http://archive.today/Sn6Hv).

[180] Executando um *full node*: https://bit.ly/3ycXP0K (arquivado: https://archive.vn/0Brfe).

[181] Distribuição global de nós do Bitcoin: https://bitnodes.io (arquivado: https://archive.vn/8RsZq).

[182] Ainda é possível rodar nó pelo TOR sem expor seu IP: https://bit.ly/3x4N8No

[183] A fabulosa ilha Bitcoin: https://bit.ly/3qBfLzr (arquivado: https://archive.vn/pvaOx).

[184] Exemplo é a transmissão de bitcoins por rádio, triangulada pela Lua, entre Márcio Gandra, Rafael Silveira, Narcélio Filho, André Alvarenga e Paulo Jr.: https://bit.ly/3hp1Bxa (arquivado: http://archive.today/CSFkJ).

[185] "Descentralizado" significa que o Bitcoin não tem autoridade ou estrutura central nem é democrático, é composto por atores independentes e a rede só decide mudanças por consenso. Caso um grupo discorde de modificação, pode continuar na versão anterior (*fork*). A rede é distribuída e descentralizada para ser antifrágil, a destruição de uma parte dos mineradores ou nós não é capaz de pará-la, todos os milhares de nós e mineradores teriam que ser destruídos simultaneamente para destruir o Bitcoin.

[186] *Money Over Internet Protocol:* imagem da Pantera Capital

[187] Bitcoin: um sistema de dinheiro eletrônico ponto a ponto: https://bitcoin.org/en/bitcoin-paper (arquivado: https://archive.vn/KmpTS)

[188] Primeiras reportagens sobre BTC em mídias convencionais foram em 2011, como essa da Globo: https://glo.bo/3qEE1jW (arquivado: http://archive.today/HLtQK). ou https://tcrn.ch/3jx9EdJ (arquivado: http://archive.today/cjofd).

[189] *Dez formas de explicar Bitcoin*: https://bit.ly/3dvZaYk (arquivado: https://archive.vn/A6WBg).

[190] *Guerra ao dinheiro*: https://bit.ly/2Tnp8Xg (arquivado: https://archive.vn/GkfEJ).

[191] Ninguém tem o poder de confiscar ou alterar transações que já aconteceram. Todas as informações estão replicadas em milhares de nós em consenso. Onde é criminalizado, pode continuar sendo transacionado com auxílio da rede TOR, VPN, com acesso físico à Internet de outra jurisdição por satélite ou qualquer meio de comunicação, como SMS, carta ou chamada discada; e, normalmente, passa a valer mais como na Venezuela: https://bbc.in/2SHUZlc (arquivado: http://archive.today/TAz26). O *spread* (ágio) no preço do bitcoin normalmente expressa custo de transação marginal derivado do controle de capitais do país.

[192] *Satoshi's quotes Re: Bitcoin does NOT violate Mises' Regression Theorem*: https://bit.ly/3AdNza5 (arquivado: http://archive.today/UtxnY).

[193] Vide: https://coinexplorer.sk/co-je-btcoin

[194] *Bitcoin Is Not Too Volatile*: https://bit.ly/2UWdROl

[195] BTC na Venezuela: https://bit.ly/2UitG11 (arquivado: https://archive.vn/S69oj).

[196] Esposa de Rocelo: https://bit.ly/3qAWQ7G (arquivado: https://archive.vn/H448F).

[197] MBL e lavagem de dinheiro: https://bit.ly/3xaDYPl (arquivado: https://archive.vn/f3HDz).

[198] Pichardo: https://bit.ly/3ymi4Ja (arquivado: https://archive.vn/W7yam).

[199] *Bitcoin as a new asset class* https://bit.ly/3Af3t4a (arquivado: https://archive.vn/NqRZL).

[200] *WTF happened in* 1971? https://wtfhappenedin1971.com/ muitos exemplos históricos são demonstrados de maneira detalhada por Mike Maloney no *Hidden Secrets of Money* e nas *Seis Lições*.

[201] *Bitcoin Revolution*: https://amzn.to/3qIzcGD

[202] *The Bitcoin Reformation - Podcast (Bitcoin Audible): The Bitcoin Reformation - by Tuur Demeester*: https://bit.ly/3jqIohc

[203] *Bitcoin and the poor*: https://bit.ly/3jxtcPk (arquivado: http://archive.today/KHr80).

[204] Mateus 5:17-19

[205] *Quantum computing and Bitcoin:* https://bit.ly/3jwp6Hi (arquivado: https://archive.vn/SBdrL).

[206] *Cryptology ePrint Archive:* https://bit.ly/3qRrcmD (arquivado: https://archive.vn/sFOam).

[207] *Is Quantum Computing a Threat to Standard Cryptocurrencies?* https://bit.ly/3qHi9Vd (arquivado: https://archive.vn/hvN29).

[208] *ENCRYPT II*: https://www.ecrypt.eu.org/.

[209] No século XIX, era comum entre trabalhadores das minas de carvão a prática de monitorar o nível de gases tóxicos usando **canários**. Esses eram primeiros a morrer, sinalizando o momento em que os mineiros deveriam deixar a mina.

[210] *Bitcoin and me*: https://bit.ly/366amqK (arquivado: http://archive.today/skZlp).

[211] Quase R$ 120 bilhões em bitcoin estão perdidos para sempre, estima empresa: https://bit.ly/3y2oCN4 (arquivado: https://archive.vn/PVDp2).

[212] É palavra adicional às 12, 18 ou 24 palavras do mnemônico (seed phrase) da carteira. Cada mnemônico pode conter inúmeras *passphrases*, formando carteiras únicas e independentes.

[213] *Dead man switch* na *Lightning Network:* https://bit.ly/2SEmpZb (arquivado: http://archive.today/QkcBm). / https://github.com/joostjager/deadmensbutton/ / https://github.com/joostjager/whatsat/tree/whatsat-paid

[214] Isso sem adiantar todos os aspectos específicos de *valuation* de criptos explicados no ponto *por que Bitcoin é o Rei?*

[215] *Gold Silver Ratio:* https://bit.ly/36428PL (arquivado: https://archive.vn/Pkbhk).

[216] *Por que Ethereum é golpe:* https://bit.ly/3w6Z6EX (arquivado: http://archive.today/5oWbA).

[217] Pré-mine do ether perpetua controle dos criadores que não colocaram 1 satoshi no projeto: https://bit.ly/3yc34Oc (arquivado: http://archive.today/7QYsl). Todos os ethers até hoje minerados não superam o pré-mine distribuído para fundadores bilionários que escolhem quais transações são válidas e anulam outras.

[218] Pesquisar sobre os casos, no Brasil, de Renné Sena e Antônio Domingo.

[219] "Ação meme" sobe 1400% em um dia:: https://bit.ly/3js9rc1 (arquivado: http://archive.today/tEBXm).

[220] *Cash and Carry:* https://bit.ly/3h5zMuQ (arquivado: http://archive.today/01Mjy).

[221] *Lending* passo-a-passo - Como receber juros usando o *Funding* da Bitfinex: https://bit.ly/2TrAF7M

[222] Atualmente, existem empresas como a *Blockfi*, que pagam 5% a.a. em *stable* de ouro, porém, o investidor incauto sofre triplo risco de custódia, perdendo tudo em caso de falha da *Blockfi* ou da *blockchain* cuja *stable* está registrada ou do emissor.

[223] Pense e enriqueça: https://bit.ly/3qIAEc3

[224] Anarquia em Pessoa: https://bit.ly/2SD5g1U (arquivado: http://archive.today/ayddq).

[225] *Social credit systems*: https://en.wikipedia.org/wiki/Social_Credit_System.

[226] A eliminação de dissidentes é uma constante em fraudes concursos e processos (assassinatos de reputação) em países bolivarianos como Venezuela e Brasil, mas começou prática pública nos EUA: Biden Administration Asks Americans to Report 'Potentially' Radicalized Friends and Family: https://bit.ly/3AgCkhe (arquivado: http://archive.today/msnjh) a ponto de dissidente da "Coreia da Morte afirmar que o ambiente acadêmico americano com sua "política de cancelamento" é tão patológico quanto a RPCD: Even North Korea is not this nuts': Defector after graduating from American university: https://bit.ly/3Air8AP (arquivado: http://archive.today/gONJ5).

[227] Pizza day 10 anos depois: https://cbsn.ws/2UhKHZb

[228] *NFT - non fungible tokens* existem amplamente desde 2016 com os "Rare Pepe" da *counter party e são registros na blockchains de imagens, videos ou textos que possam ser considerado arte em si mesmos ou prova de propriedade de arte ou outro ativo: NFTs History — From Rare Pepe to Beeple 69 Million Dollar NFT sale:* https://bit.ly/3w6LJ7S *(arquivado: http://archive.today/aPaOG).*

[229] A arte de sonegar: Como milionários usam obras de arte para evitar serem roubados: https://bit.ly/3DoRiDA

[230] *NFTs are Doomed:* https://bit.ly/3h7Zoat (arquivado: http://archive.today/dlHH3).

[231] *NFT* na Liquid: https://elixir.app/

[232] 6 leis de maca: https://twitter.com/noshitcoins/status/1427081434385297415

[233] Com o gabarito e a punção da *stackbit*, ou agulha/prego, também pode furar cartão de crédito/plano velho de plástico, ainda mais discreto, para passar na carteira sem chamariz em metal.

[234] *Plausible Deniability*: https://bit.ly/3xhURrE

[235] Uma ENORME oportunidade judicial existe em responsabilizar o *YouTube/Google* por receber dinheiro de bandidos para anunciar falsos *giveaways*, até mesmo permitindo que robôs fraudem número de curtidas/*views*. O google não é apenas negligente em sua "*due diligence*", como também mama no dinheiro roubado. Eficiente para banir "discurso de ódio" (ideologia contrária a deles) e incapaz de retirar do ar anúncios oficiais de crimes, com os quais eles lucram às custas das vítimas.

[236] *Known Physical Bitcoin Attacks:* https://bit.ly/3AnQmh3

[237] *How to Protect Your Bitcoin from $5 Wrench Attacks:* https://bit.ly/2UhLR6Z (arquivado: http://archive.today/j7wZJ).

[238] *Visions of Bitcoin:* https://bit.ly/3x40XM5 (arquivado: https://archive.vn/3bUve).

[239] Visions of Bitcoin: https://bit.ly/3h7W6Eb

[240]*Why Bitcoin is the Key to Abundance:* https://bit.ly/3AtgEOO

[241] Uma entrevista com F. A. Hayek – 1984: https://bit.ly/3qASzBo (arquivado: https://archive.vn/h1XMz).

[242] Milton Friedman prevê bitcoin em 1999: https://bit.ly/2SPflsO

[243] Peter Thiel prevendo bitcoin em 1999: https://bit.ly/3wc4XJ4

[244]Problema dos dois generais: https://bit.ly/3yjerUh

[245] Ordem cronológica com um link para mais informações detalhadas sobre o gráfico: https://bit.ly/2SLNFVH (arquivado: https://archive.vn/ytlPv).

[246] Fonte: *Money transformed - The future of currency in a digital word F&D - Finance and Development – June 218 FMI- Internacional Monetary Fund:* https://bit.ly/3heT0y3

[247] Nick Szabo, *The History of Money:* https://bit.ly/3wgVQqs

[248] Nick Szabo, *Shelling Out: The Origins of Money:* https://bit.ly/3hfvD7K (arquivado: http://archive.today/e8igf).

[249] Comércio é troca voluntária que eleva valor, em regra, se uma pessoa vende um bem por R$1, para o vendedor ele vale menos de R$1 e para o comprador mais de R$1 - e ambos saem subjetivamente mais ricos da transação.

[250] Degeneração das repúblicas. CAESARISM: THE DECLINE OF THE WEST: https://bit.ly/3dGkvyr

[251] Compra de poder estatal para produção de decisões, políticas e leis para seu benefício direto, como Elon Musk*: Debunking Elon Musk* (a parte 2 é ainda melhor para entender seu histórico fraudulento): https://bit.ly/36c9VeA

[252] *Double eagle:* https://bit.ly/3jTzZTR

[253] 2000 réis: https://bit.ly/3jC2lSh

[254] Fonte: @BTCTimeTraveler *(Twitter).*

[255] Fonte: @anilsaidso *(twitter).*

[256] *Japan central bank loses billions on ETFs, may face annual loss*: https://reut.rs/3x8KXbJ (arquivado: https://archive.vn/3AWTA).

[257] *Swiss Central Bank Holds $129 Billion in Equities, Owns More Public Shares of Facebook Than Zuckerberg:* https://bit.ly/3hkupHa (arquivado: https://archive.vn/gx5TT).

[258] *Debt Traps*, projetos chineses economicamente inviáveis usados como “armadilhas de dívida” para controlar a infraestrutura fundamental e a finanças de países controlados, incluem construção de cidades inteiras no Egito (*NAC*), Indonésia (*Jokograd*), Malásia (*Forest City*) e a Ponte de Itaparica.: https://bit.ly/3wkplrA

[259] *Central banks balance sheets for the BoJ, ECB, Fed, SNB and BoE:* https://tmsnrt.rs/367qrMC (arquivado: http://archive.today/MddeJ).

[260] *Only One Number Mattered to Global Markets in 2020:* https://bit.ly/3AfTWtB (arquivado: http://archive.today/6q8I3).

[261] *1929 versus now: are we headed for the greatest depression?* (Mike Maloney): https://bit.ly/3hdVpZW

[262] O Bug do ouro: https://bit.ly/3ycxPm4 (arquivado: http://archive.today/VYvvw).

[263] Na Venezuela o bitcoin tem ágio altíssimo e ouro não vale nem metade. Ouro sintético colateralizado por cripto já é algo superior a ouro físico em vários aspectos: pode ser facilmente verificado, capitalizado, usado como colateral, alugado e enviado pela Internet.

[264] *Ford Quote:* https://bit.ly/36dtUcO

[265] Carl Menger, "pai da Economia Austríaca", estruturou a vendabilidade através do tempo (durabilidade), espaço (transportabilidade) e escala (divisibilidade): *[THREAD BITCOIN STANDARD*] @MisesCapital (twitter): https://bit.ly/3dz2B0C (arquivado: http://archive.today/iWk9s).

[266] Golpe de bilhões: https://bit.ly/3xlzbuE (arquivado: http://archive.today/ijUUF).

[267] [THREAD OURO - RESERVA DE VALOR]: @rothbarbara (*twitter*)

A desmonetização do Ouro vem sendo desde seu último *rally* na década de 80: https://bit.ly/3AiII7N (arquivado: http://archive.today/3kbr9).

[268] Empréstimo colateralizado em real a partir de 0.69%am: https://rispar.com.br

[269] *Originalmy*: https://originalmy.com

[270]Considerando XAU, onça troy, 31,1035g, a 2000 USD: https://8marketcap.com

[271] Ouro compra 1 leva 2: https://bit.ly/2UVqedf (arquivado: https://archive.vn/K4ePg).

[272] 83 Toneladas em ouro falso em bancos: https://bit.ly/3AdjSpI (arquivado: https://archive.vn/X6d8w).

[273] *World Gold Council*: https://www.gold.org/about-gold

[274] *Venezuela's Bitcoin Birth Proves Crypto Beats Gold in Hyperinflated Economy:* https://bit.ly/3y8qpAc (arquivado: https://archive.vn/x3ySL).

[275] A unidade nativa da Lightning Network é o milissatoshi, equivalente a 0,001 satoshi ou 0,00000000001 BTC (onze casas decimais).

[276] *The Bullish Case for Bitcoin:* https://bit.ly/2UQWnm5 (arquivado: https://archive.vn/K9Knq).

[277] *S2F: Stock to Flow.*

[278] *Para comparar retornos e índices de ativos em BTC:* https://www.microstrategy.com/en/hyperintelligence/asset-vs-btc

[279] Dalio prefere BTC a títulos, que seriam "perda fixa": *Bridgewater's Ray Dalio Says He Prefers Bitcoin to Bonds:* https://bloom.bg/3Aq9DP9 (arquivado: http://archive.today/SgJpT) bitcoin é um ativo com baixa correlação com demais mercados e altos índices de retorno descontados do risco, capaz de elevar lucratividade potencial na composição de carteiras.

[280] Em junho de 2021, Paul Tudor Jones passa a recomendar não 1%, mas agora 5% da carteria em Bitcoin: https://bit.ly/3ymT1p9 (arquivado: http://archive.today/o5r4l)

[281] Como o Bitcoin força o consenso entre os generais bizantinos? https://bit.ly/3w6YOy0 (arquivado: https://archive.vn/cy625).

[282] Falha Bizantina, o que significa? https://bit.ly/3htUCTM (arquivado: https://archive.vn/fG55a).

[283] Prova de trabalho, *Proof-of-Work* (*PoW*). Uma parte de um dado que requer um esforço computacional considerável para ser encontrada. No Bitcoin, mineradores devem encontrar uma solução numérica para o algoritmo SHA-256 que esteja em conformidade com os parâmetros da rede.

[284] Efeito Lindy: https://pt.wikipedia.org/wiki/Efeito_Lindy

[285] Efeito rede: https://pt.wikipedia.org/wiki/Efeito_de_rede

[286] Lei de Gall: http://principles-wiki.net/principles:gall_s_law

[287] Compilação dos melhores links para artigos desmascarando Bitcoin FUD: https://endthefud.org/

[288] *Thirst Trap:* https://bit.ly/36fcX1z

[289] Bitcoin's energy use compared to other major industries: https://bit.ly/3gASSse (arquivado: http://archive.today/ypSeo)

[290] *Bitcoin Energy Consumption Index:* https://bit.ly/3hB2jHs (arquivado: https://archive.vn/WslVC).

[291] *Bitcoin energy use - mined the gap*: https://bit.ly/3hA5YXP (arquivado: http://archive.today/T02oB)

[292] LN 3,7M mais eficiente que VISA: https://bit.ly/2SFtAAn (arquivado: http://archive.today/7GuGT).

[293] *Bitcoin and ESG*: https://bit.ly/3hiPKR8 (arquivado: http://archive.today/7OYuw).

[294] *ESG = Energy Stops Growing*: https://bit.ly/2Ue6KjN (arquivado: http://archive.today/GQfZ7).

[295] 30 anos de *economic warfare* chinês contra ocidente / *Panic As Chinese Skyscraper Wobbles!:* https://bit.ly/2WuzlT9

[296] *Superdollars* da Coréia da Morte / *When North Korea tried to hijack the US dollar*: https://bit.ly/3dG1FHK

[297] Até mídia esquerdista especula se COVID foi fabricada: https://on.wsj.com/3h986oG (arquivado: http://archive.today/1ICtP).

[298] Teoria Crítica Racial e marxismo até nas forças armadas: https://youtu.be/1814HNjVntA

[299] *COVID BIO WEAPON*: https://bit.ly/3x9D9qg *(youtube) /* *Wuhan Coronavirus Lab Leak No Longer a "Conspiracy Theory":* https://bit.ly/3w9ukvk

[300] OMS mentiu dolosamente: *The WHO Knowingly Lied About China:* https://bit.ly/3jyMhkm

[301] Comer carne salva planeta: *Eating less Meat won't save the Planet. Here's Why*: https://bit.ly/3hoxKF4 há tréplica também neste canal a todos os argumentos mentirosos dos ativistas.

[302] Imagens de Bill Gates com mama *(man boobs)* e culote *(love handles*): https://bit.ly/3wb6GP5 (arquivado: http://archive.today/ldcQd).

[303] Focinheiras insalubres e inseguras: https://bit.ly/3AbJDXo (arquivado: http://archive.today/udjs3).

[304] Declaração de Barrington: https://bit.ly/3wbfG6K (arquivado: http://archive.today/ti8fZ).

[305] *Michael Bedford Taylor, University of Washington*: https://bit.ly/2UXJTt3 (arquivado: https://archive.vn/dz0AG)

[306] *Dhruv Bansal*: https://bit.ly/2UXJTt3 (arquivado: https://archive.vn/dz0AG) e https://bit.ly/3h6MqJU (arquivado: https://archive.vn/Glj17)

[307] Gigante norueguesa no setor de petróleo e gás, presidida por Kjell Inge Røkke, um dos dez homens mais ricos da Noruega.

[308] Cartas aos investidores da AKER: https://bit.ly/2V21ss5

[309] *Whitepaper* da Square sobre energia e Bitcoin: https://bit.ly/366Kqva

[310] *Bitcoin Clean Energy Initiative*: https://squ.re/3ktrTzJ (arquivado: http://archive.today/RsbuW)

[311] *A Closer Look at the Environmental Impact of Bitcoin Mining:* https://bit.ly/3uY8ET1 (arquivado: http://archive.today/vB2bU)

[312] *On Bitcoin`s Energy Consumption: A Quantitative Approach to a Subjective Question*: https://bit.ly/3hwHfDP (arquivado: http://archive.today/NHn8M).

[313] Crise energética no Texas: https://bit.ly/3jLNJzX

[314] Lado sombrio da energia solar: https://bit.ly/2Tifu8r (arquivado: http://archive.today/vNTGg).

[315] Usualmente inconstante em sua produção, como solar e eólica.

[316] Desastre alemão: https://bit.ly/3Alrh6g (arquivado: http://archive.today/BspBI).

[317] *Safely Managing Used Nuclear Fuel:* https://bit.ly/3fpK9Yh (arquivado: http://archive.today/tZxf8).

[318] *5 Fast Facts about Spent Nuclear Fuel:* https://bit.ly/3orWhvP (arquivado: http://archive.today/ZhnAW).

[319] *Novaterra*: https://cnb.cx/3juCFa9 (arquivado: http://archive.today/hl6v0).

[320] O *"The Great Reset"* é uma versão reformulada e restrita da agenda de “Desenvolvimento Sustentável” de décadas da ONU (“Agenda 21“): https://bit.ly/3wmPmGE (arquivado: http://archive.today/zu96e). As mesmas políticas e ideias estão contidas no *“The Green New Deal”*, que foi reprovado em 2019 no Congresso dos EUA: https://bit.ly/36iPvAo (arquivado: http://archive.today/Pys9Y).

[321] Fórum Econômico Mundial (FEM) em conjunto com as Nações Unidas (ONU) e o Fundo Monetário Internacional (FMI) / *Meet the World Economic Forum:* https://bit.ly/36ls6yp

[322] O Grande Reset Financeiro Mundial: https://bit.ly/3jKvvyG

[323] Afinal, qual é a desse “Grande Reinício”? https://bit.ly/3dPOAvk (arquivado: http://archive.today/8O8Yg).

[324] Globalista Klaus Schwab: O mundo “nunca” voltará ao normal depois do COVID-19: https://bit.ly/36e7p7w (arquivado: http://archive.today/PDp1p).

[325] *Bitcoin Address:* https://en.bitcoin.it/wiki/Address (arquivado: https://archive.vn/uBmN6).

[326] Para Chaves, Endereços e Carteiras no Bitcoin: diferença entre Chave Pública e Endereço, ver o artigo no *medium* da Rafaela Romano: https://bit.ly/2UfqR10 (arquivado: https://archive.vn/ljQxw) e https://medium.com/@rafaelaromano.

[327] *BIP - Bitcoin improvement proposal* (Proposta de Melhoria do Bitcoin) é um documento para a introdução de novos recursos ou informações no Bitcoin.

[328] Unidades de medida: https://bit.ly/3jFmHdf (arquivado: https://archive.vn/fWidk)

[329] A circulação total em abril de 2019: https://coinmarketcap.com em 27/04/2020

[330] Blog do Nick Szabo: https://bit.ly/3qFZngZ (arquivado: https://archive.vn/454kk).

[331] *Money, blockchains, and social scalability:* https://bit.ly/3hoAthB (arquivado: https://archive.vn/454kk).

[332] *Opendime*: https://opendime.com

[333] *Stackbit*: www.stackbit.me

[334] Acompanhe a "Serie bugs do Bitcoin": https://bit.ly/38eyto4 (Canal do youtube Safersr apresentado por Peter Turguniev, entender a historia dos problemas do Bitcoin e como o a rede tem a capacidade de atrair as maiores mentes do mundo da programação para manter tudo isso "de pé".

[335] Bug de inflação *(CVE-2010-5139)*

[336] *Bitcoin History Part 10: The 184 Billion BTC Bug* (CVE-2010-5139): https://bit.ly/3wm4sfJ (arquivado: http://archive.today/UXsTW).

[337] Duas horas depois da ocorrência do *Common Vulnerability and Exposure 2010-5139*, os desenvolvedores do Core Gavin Andresen e Satoshi Nakamoto estavam no caso, e a transação de 184 bilhões de BTCs foi eliminada do bloco 74638.

[338] Quanto custa fazer um ataque de 51% em cada criptomoeda que utiliza o *PoW:* https://www.crypto51.app/

[339] https://www.bitcoinblockhalf.com/

[340] Gráficos de BTC desde sempre em prata, ouro, US$ e índices disponíveis em *Asset gallery*: https://asset.gallery

[341] Mesquitas de Mamón: https://bit.ly/3wivxQV

[342] Tutorial/experiência de como minerar em casa - *Home mining for non-KYC Bitcoin: https://bit.ly/3mDgpws* (arquivado: http://archive.today/HY2fL)

[343] *HODL*: https://bit.ly/3x5YDUR

[344] Satoshi na época chegou a se opor a *Wikileaks* aceitar BTC, imagine uso por *Silk Road.*

[345] IN 1888/2019: https://bit.ly/3dB9MFz (arquivado: https://archive.vn/kIuuE).

[346] Calculadora do preço médio: https://dcabtc.com

[347] Preço médio de compra, bitcoins dormentes por dia, saldos líquidos em corretoras, *hashrate* e valor movimentado por dia são indicadores (mesmo que consequentes) dos fundamentos do BTC.

[348] Crédito em Reais com garantia em bitcoin: https://rispar.com.br/

[349] Cotações do *lending*: https://defirate.com/btc/

[350]*Skew*: https://analytics.skew.com/

[351] *Florida Teenager Is Charged as 'Mastermind' of Twitter Hack:* https://nyti.ms/3dxK8BB (arquivado: https://archive.vn/WUIBP).

[352] *Colonial Pipeline* paga 90 milhões em *ransom* para nada: https://bit.ly/3AeuKnr (arquivado: http://archive.today/kCZ48).

[353] *Wannacry*: https://glo.bo/3h9V8Y3 (arquivado: https://archive.vn/XzPpJ)

[354] *Wannacry wiki*: https://bit.ly/3h7BOKY

[355] Por que os bancos centrais poderiam emitir moedas digitais? https://bit.ly/3hc12Yo (arquivado: http://archive.today/WhwOD).

[356] Como o advento do Bitcoin pode influenciar o pensamento dos Bancos Centrais: https://bit.ly/3wh6xcY (arquivado: http://archive.today/qXU0J).

[357] *The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies*: https://bit.ly/3h6Yz1s (arquivado: http://archive.today/87Xup).

[358] *FED AND UN think CBDC could kill Banks:* https://yhoo.it/3hs4BsE (arquivado: http://archive.today/fC7GJ).

[359] O fim dos bancos como conhecemos: https://bit.ly/3dPTfOd

[360] “Teimosinha" é a busca automática de ativos nas contas do devedor de forma contínua: https://bit.ly/3h9WulF (arquivado: http://archive.today/7qjoO).

[361] Vide as 10 medidas nazi stalinistas, amplamente defendidas por órgãos aparelhados e militantes, como MPF: https://bit.ly/3y5iHqy (arquivado: http://archive.today/nwMfA).

[362] Arthur Hayes sobre juro negativo e cenários futuros: https://bit.ly/3duqK8v

[363] *MPEX* (*Mircea Popescu Exchange) em 2011 já provava como se poderia negociar futuros, commodities, opções e síntéticos de moedas e ações - embora o site fosse apenas um prova de conceito e os volumes fossem pífios:* http://mpex.biz/faq.html

[364] *Satoshi Dice*: https://en.bitcoin.it/wiki/Satoshi_Dice

[365] *Piper Wallet* de 2015 gerava e imprimia chaves *offline*: https://bit.ly/3hgE4Qg *hardware wallets* mais modernas como MK3 da *Coldcard* geram transações *offline*.

[366] BOLSONARO2022: https://bit.ly/3haDsLP (arquivado: http://archive.today/GpPrj).

[367] Solução de mercado para libertar a Venezuela: https://bit.ly/3sOr3RO (arquivado: http://archive.today/dXojH)

[368] Candidato no Brasil a ser o *APP* oficial é o *Nubank* que conta com participação do *deep state* e da ditadura chinesa desde 2018 através da *Tencent* (dona do WeChat)

[369] Utilize o site https://hive.one, um serviço que faz um *rank* sobre as principais personalidades do mundo *crypto.*

[370] *DYOR* entre Posteo, Protonmail, Tutanota e outros: https://zapier.com/blog/secure-email/

[371] Democratas já tem listas públicas para expurgos e reeducação: https://bit.ly/3hpLFut (arquivado: http://archive.today/8gXFG).

[372] *"Como o governo e as big techs* estão doutrinando você” : NOVO, Bolsonaro e “moderados” são instrumentos progressistas: https://bit.ly/3hbiah8

[373] *Everything bubble*: https://bit.ly/2Ugmd2F

[374] *Financial markets:* https://bit.ly/2Uk3O51

[375] *Dissection of Bitcoin’s multiscale bubble history:* https://doi.org/10.1098/rsos.180643 (arquivado: https://archive.vn/trmp9).

[376] Lei de Metcalfe: https://bit.ly/3jCCidG

[377] *Aimstone explica estimativa de Breedlove:* https://bit.ly/3wfIH14

[378] Gráfico atualizado diariamente (@Ecoinometrics): https://ecoinometrics.substack.com/

[379] Ouro a 50k USD em 2022 /
Can Gold Hit $50,000 By 2022? (Expert Says YES!): https://bit.ly/3qMtQdy

[380] 5 fases do BTC: https://bit.ly/3wcPMiK

[381] Peter Thiel afirma que bitcoin é arma estratégica e roga que EUA pare de vender os *tokens* apreendidos: https://bit.ly/3jvaibX (arquivado: http://archive.today/c9kMi).

[382] *Tether Dollar, USDT:* https://bit.ly/3hsbHxi

[383] CME manipulation: https://bit.ly/3qEQTqs

[384] Mercado provocando maximum pain no varejo: https://bit.ly/3w5hv52

[385] Considerando XAU a 1900 USD.

[386] *All the world's money and markets in one visualization*: https://bit.ly/3hadMyN (arquivado: https://archive.vn/7Ee0I) só para se ter uma noção de como esses números estão defasados e a impressão de moeda medonha, nessa publicação (maio de 2020) existiam 2095 bilionários, em maio de 2021 já eram 2755, segundo o *ranking* da Forbes: https://bit.ly/3dRYSvl

[387] Estimativas indicam mais de 199.000 toneladas de ouro em 2019: https://bit.ly/3wdernv

[388] Inflação do ouro em 2,5% aa na década: https://bit.ly/3jDhrXB (arquivado: http://archive.today/X5xGU) e inflação do bitcoin em 2021 é de 1,8%.

[389] Conta detalhada: https://bit.ly/3AdiQKt

[390] Quantos satoshis existem por pessoa no mundo? https://satoshisperperson.com/

[391] 24 (horas por dia) * 6 (blocos por hora) * 6,25(BTC por bloco)

[392] *Grayscale's 654,885 BTC:* https://bit.ly/2UPhh52

[393] Entidades que possuem bitcoin em seus balanços: Bitcoin Treasuries: https://www.buybitcoinworldwide.com/treasuries/

[394] *Tesla still has 38300 BTC*: https://bit.ly/2ToZcdG

[395] *Gartner Hype Cycle:* https://www.gartner.com/en/research/methodologies/gartner-hype-cycle

[396] *Bitcoin is not too volatile:* https://bit.ly/3zs7bqq

[397] *Bitcoin Price Forecast:* https://bit.ly/2TuzLHH (arquivado: https://archive.vn/5Hlim).

[398] *Podcast* de Stephan Livera: https://stephanlivera.com/episode/2/

[399] Lei de Gresham: https://bit.ly/3jDlK5d (arquivado: https://archive.vn/l5co6).

[400] 5 fases do BTC: arquivado: http://archive.today/NZp7q

[401] GBTC | Grayscale Bitcoin Investment Trust: https://grayscale.com/products/grayscale-bitcoin-trust/

[402] *Ranking* de empresas que estão entesourando bitcoins:
https://bitcointreasuries.org/

[403] QBTC11 ou HASH11? https://bit.ly/3AnUgqd

[404] Psicologia dos Ciclos emocionais de Mercado: https://bit.ly/3dIXZ7Y (arquivado: https://archive.vn/DihRt).

[405] *Mayer multiple:* https://mayermultiple.info/

[406] *Stock to Flow*: https://bit.ly/3hzDn3c

[407] Bitcoin em 2020 é Internet em 1997: https://bit.ly/3qDl7Kq

[408] *Hyperbitcoinization:* https://bit.ly/3AjqS4A (arquivado: https://archive.vn/4P085).

[409] Super ciclos: https://bit.ly/3dGFsJA

[410] Um problema atual é o excesso de crédito, a maioria das grandes empresas hoje são zumbis: só existem graças a juro negativo. Se o juro subir ao normal histórico, muitas empresas somem.

[411] Volatilidade do bitcoin está menor no *halving*: https://bit.ly/3xcYn6C (arquivado: https://archive.vn/JsXwl).

[412] *Programming Bitcoin: https://amzn.to/3Auqbpc*

[413] *@real_vijay Twitter*.

[414] Debates e *roadmaps* históricos: https://bit.ly/3h70JOO (arquivado: https://archive.vn/sNHXb).

[415] *Bitcoin Roadmap to 2025*: https://bit.ly/3dx8n2w

[416] *Github*: https://bit.ly/3AdpDUt

[417] *BITCOIN BIPs* https://github.com/bitcoin/bips

[418] *Blockstream*: https://blockstream.com/

[419] *Liquid*: https://liquid.net/

[420] *RSK*: https://www.rsk.co/

[421] O que está acontecendo no ecossistema Lightning Network: https://bit.ly/3gYiboj (arquivado: http://archive.today/3s2pP)

[422] Fonte: inmainnet – malhas da rede LN. / Acompanhe o crescimento - *Lightning Network Search and Analysis Engine:* https://1ml.com/

[423] https://bit.ly/3sTnf1T

[424] *Schnorr signature:* https://bit.ly/3yfXsSM

[425] *Taproot Is Coming: What It Is, And How It Will Benefit Bitcoin:* https://bit.ly/2Tr5Xf9 (arquivado: https://archive.vn/jmELU).

[426] *What is the Bitcoin Taproot upgrade?* https://bit.ly/3jHXO0r (Taproot uses a structure called Merkelized Abstract Syntax Trees)

[427] Fungibilidade é o atributo pertencente aos bens móveis que podem ser substituídos por outros da mesma espécie, qualidade e quantidade. Ex.: O dinheiro é o bem fungível por excelência, dado que, quando se empresta uma quantia a alguém (por exemplo, R$100,00), não se está exigindo de volta aquelas mesmas cédulas, mas sim um valor que pode ser pago com quaisquer notas de Real (moeda).

[428] Trilema da escalabilidade: https://bit.ly/3wgAyJC

[429] *Finney Bitcoin banks*: https://bit.ly/3ycUzSP

[430] *Nick Szabo btc layers (twitter):* https://bit.ly/365H2jV

[431] *Lightning Network Search and Analysis Engine: https://1ml.com/*

[432] Os 195.875 WBTC nem consideramos na conta nem os *wrapped BTC em outras redes como Tron que só aumentam as distorções do coin market cap* para arguir pela "perda de dominância". A busca de *tokens* sintéticos em *shitcoins* para economizar em custos de transações representa riscos operacionais compostos - ganhar de colher para perder de balde.

[433] *Drivechain:* https://www.drivechain.info/

[434] *Statechains:* Non-custodial Off-chain Bitcoin Transfer: https://bit.ly/3hnuZUt

[435] *Private & scalable smart contracts for Bitcoin and Lightning Network:* https://rgb-org.github.io/

[436] Impervious: https://www.impervious.ai/

[437] *Stacks:* https://www.stacks.co/

[438] https://twitter.com/100trillionUSD.

[439] https://medium.com/@100trillionUSD.

[440] *Fermions Flows (FF) Whale Model:* https://bit.ly/3qH4ihN (arquivado: https://archive.vn/qNLEo).

[441] Comparações e definições *(Bitcoin Price Models*): https://bit.ly/3dF8xFp

[442] *Bitcoin price and its marginal cost of production:* https://arxiv.org/pdf/1805.07610.pdf

[443] Ray Nasser – China e seu erro de 1 trilhão de USD: https://bit.ly/3Do6P6o

[444] *Bitcoin's Cost of Production: https*://bit.ly/3sVfZCo

[445] *Bitcoin Price Forecast: https://bit.ly/3qHftXz* (arquivado: https://archive.vn/5Hlim).

[446] Fonte: www.visualcapitalist.com

[447] https://99bitcoins.com/bitcoin-obituaries/

[448] Quais os Impactos da Computação Quântica para os Bitcoins: https://bit.ly/36acHkp (arquivado: https://archive.vn/WZpH9).

[449] Fonte: www.administradores.com.br

[450] Talibã significa "estudante", para quem tiver dúvidas de que instrução formal não "melhora" pessoas intelectual ou moralmente. *Origins of Taliban:* https://www.youtube.com/watch?v=zzBVvyBWDD4 O Antigo Testamento já reconhecia que "estudar demais é enfado" e que "não há limites para fazer livros" (papel aceita tudo), no Eclesiastes 12:12.

Table of Contents